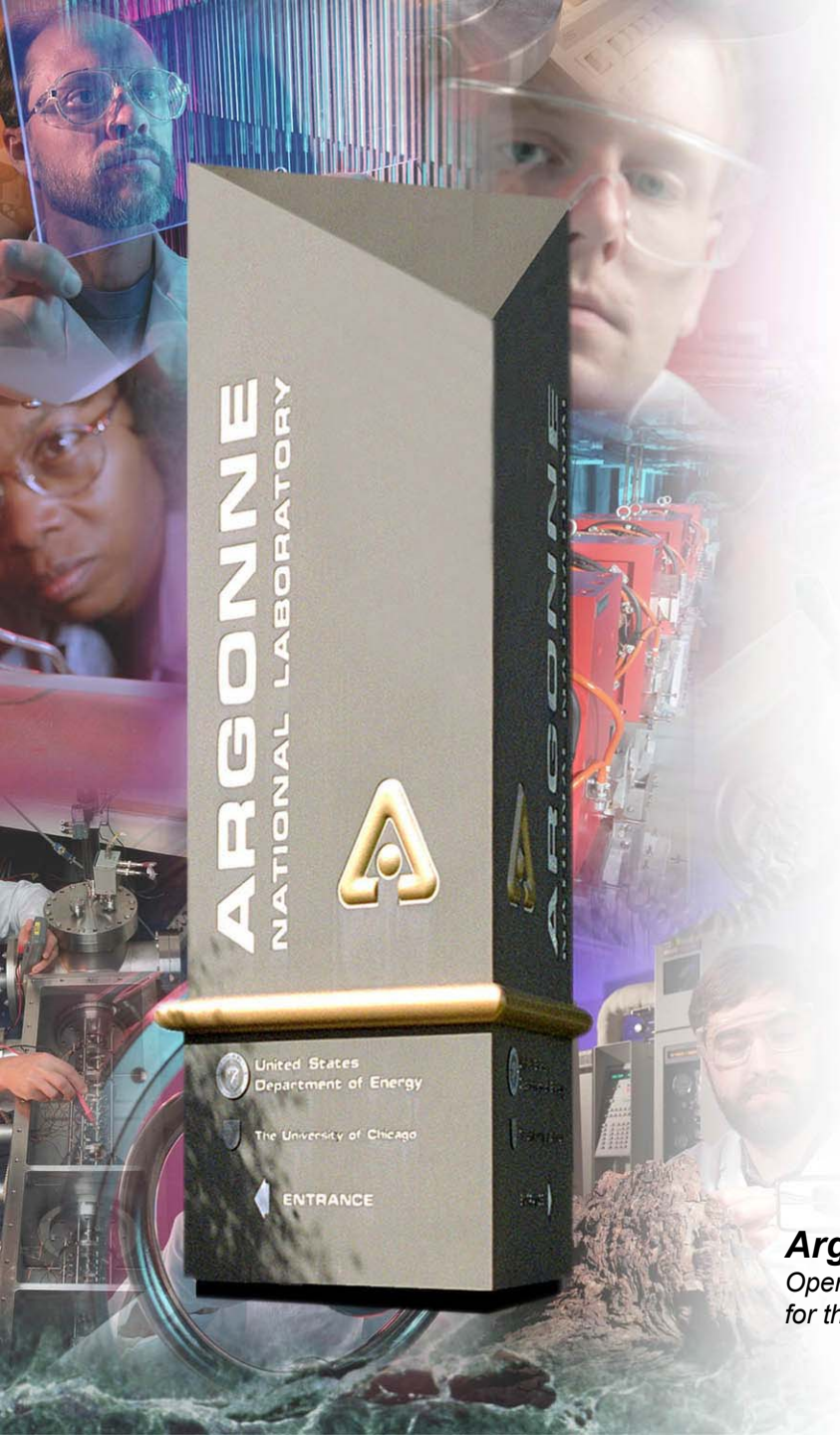
Talk Notes

This talk was delivered at the Large Installation System Administration 2003 conference in October, 2003. It is meant to be a frank, and sometimes humorous, description of the Argonne cybersecurity activities from 2001 to 2003. The audience was technical and well-versed in practical cybersecurity issues.

These slides describe the project from my own perspective, based on a great deal of input from my co-authors. There are many viewpoints on the project, and not everyone who was involved in it will have the same perspective on all topics. However, I do believe we will all agree on one point that I made clear in the presentation – this project was a success because a large number of people from all over the Lab – security representatives, security professionals, and the project team – worked hard and worked together on this.

Remy Evard, October 2003



Security versus Science

Changing the Security Culture of a National Laboratory

Rémy Evard – evard@mcs.anl.gov

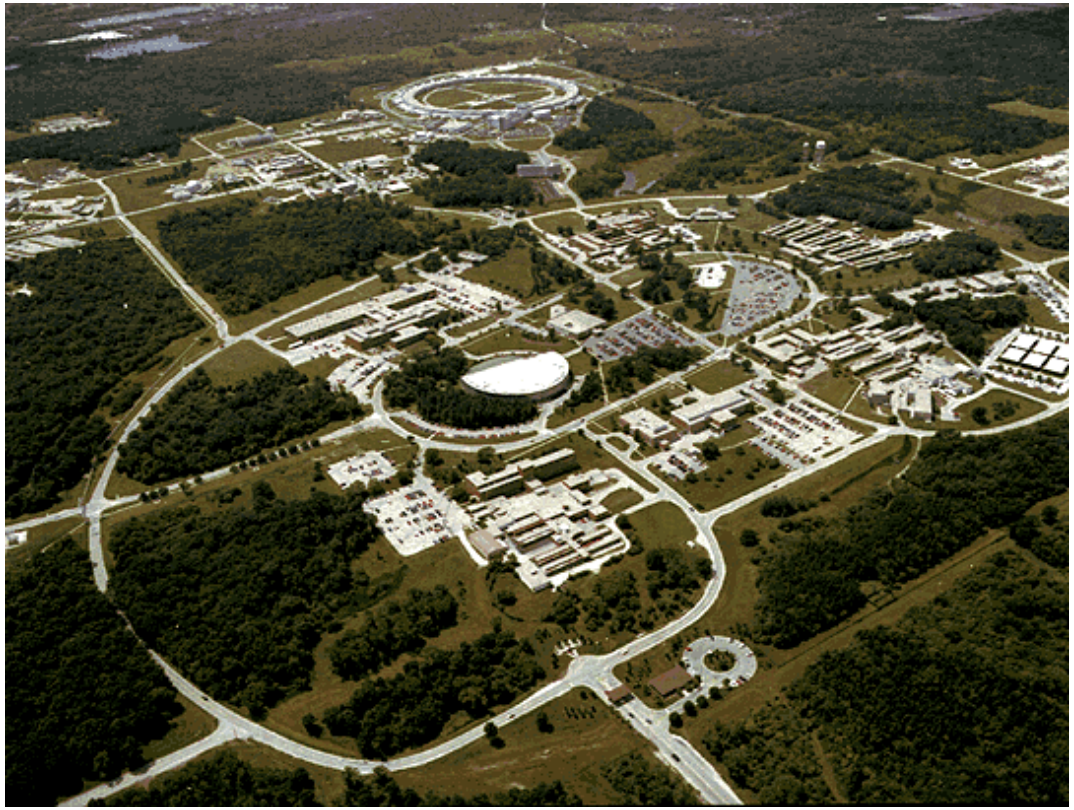
Deputy Division Director
Mathematics and Computer Science Division
Argonne National Laboratory

Co-Authors:

Scott Pinkerton, CIS
Mike Skwarek, CIS
Gene Rackow, MCS

Argonne National Laboratory
Operated by The University of Chicago
for the U.S. Department of Energy

Argonne National Laboratory

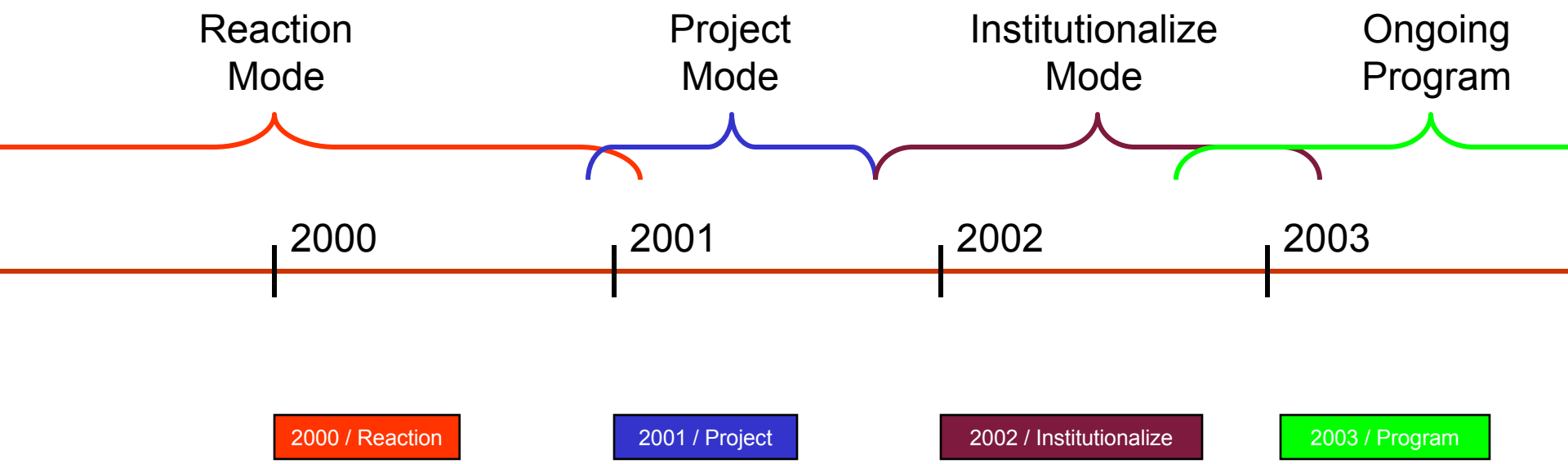


Argonne is one of 15 National Laboratories that are run by the Department of Energy. Argonne is operated for the DOE by the University of Chicago.

- www.anl.gov
- 2 campuses:
  - Chicago
  - Idaho
- ~5000 employees
- Focus areas:
  - Many different kinds of science, engineering, and scientific facilities: physics, materials, mathematics, biosciences, etc.
  - The Advanced Photon Source.
  - Energy Sciences and research.

- The activity described here only relates to the *unclassified* programs.

ANL Cybersecurity Timeline



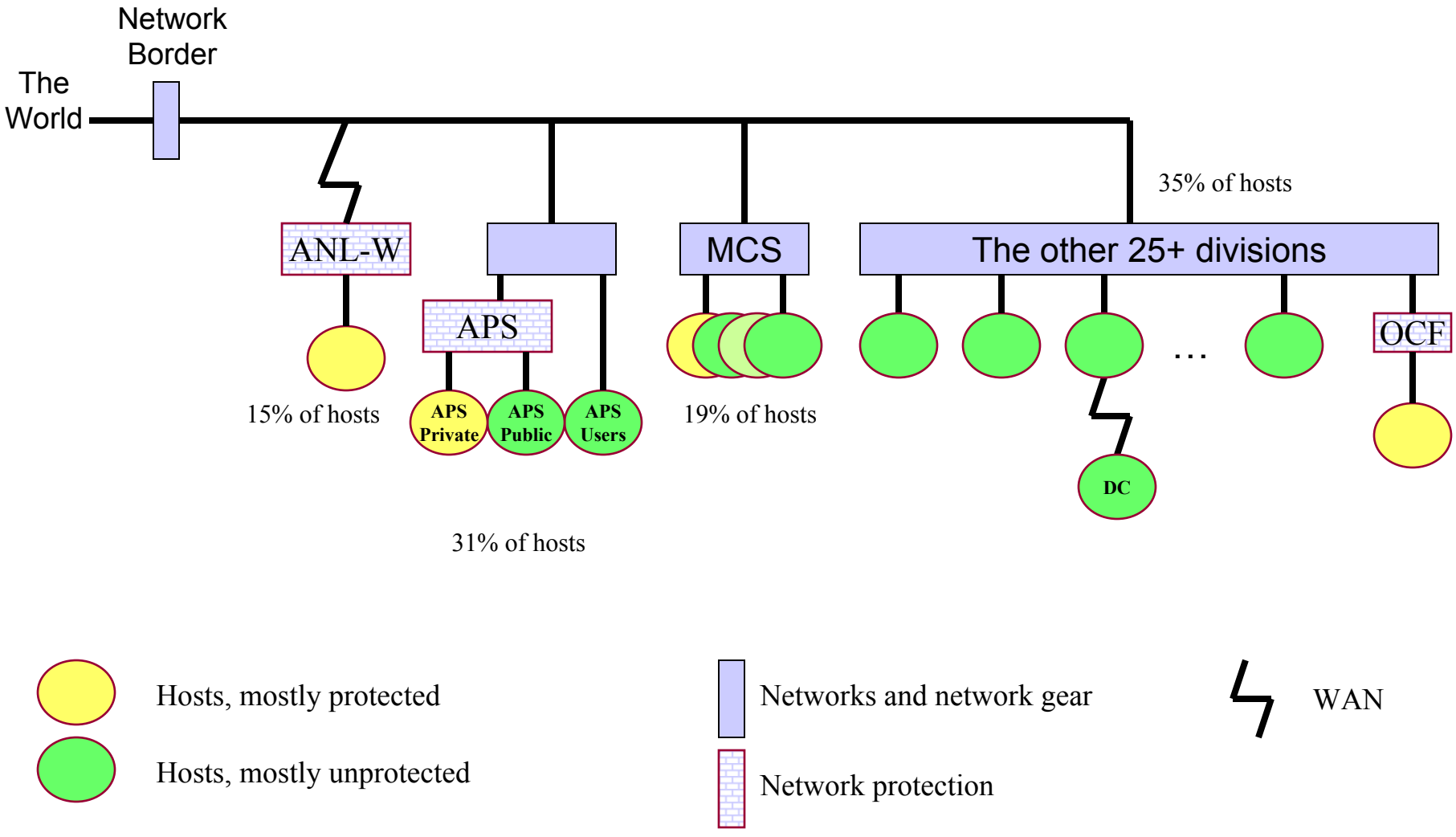
Reaction Mode – up through early 2001

- No management support for security.
- No real lab-wide security policy mechanism – or policies.
- No lab-wide security strategy or infrastructure.
- Some divisions cared about security, some did not.

- Inconsistent security.
- High security incident rate.
  - 23 reported intrusions in 1998, 17 in 1999, 13 in 2000.

The Laboratory Network – Conceptual

2000 / Reaction



Example of Trying to Set Lab-wide Policy

2000 / Reaction

- The use of "clear-text passwords" is a known security problem.
  - Technical alternatives have existed for several years.
- MCS and APS restricted their networks from clear-text passwords over a year ago.
- During the cybersecurity audits, ECT managers decided it was important to protect the entire lab from clear-text passwords.
  - Proposals to do so, created by ECT, were brought before CIPC several times, with no clear decisions.
  - Eventually the question was passed on to the "ANL Network Managers", a technical coordination group.
  - The network managers responded for each of their divisions with various issues. A technical implementation was developed over a period of six months.
  - After developing a sort of general consensus among network managers, the policy was implemented on the border routers.
  - Much later, a DD/DH memo came out, formally stating the policy.
  - Even at present, large sections of the lab are exempt from the policy.

This slide is from an internal report written in Dec 2000.

Pressure Builds

2000 / Reaction

- January 2000 – The General Accounting Office of Congress (GAO)
  - 75 Findings
- August 2000 – DOE's Office of Independent Oversight and Performance Assessment (OA)
  - 17 Findings
- October 2000 – The Lab's prime contract is amended to include security measures.
- March 2001 – The OA returns
  - 7 Findings
    - "Finding: CH-2001-ANLE-CS-1. ANL-E has not established a cyber security risk assessment process to fully identify, evaluate, and address threats to the network."
    - No lab-wide direction.
    - Failure to follow DOE Orders on passwords, foreign nationals, and banners.
    - No network perimeter.
    - Open modems.
    - No configuration management.

The Root of the Problem - Culture

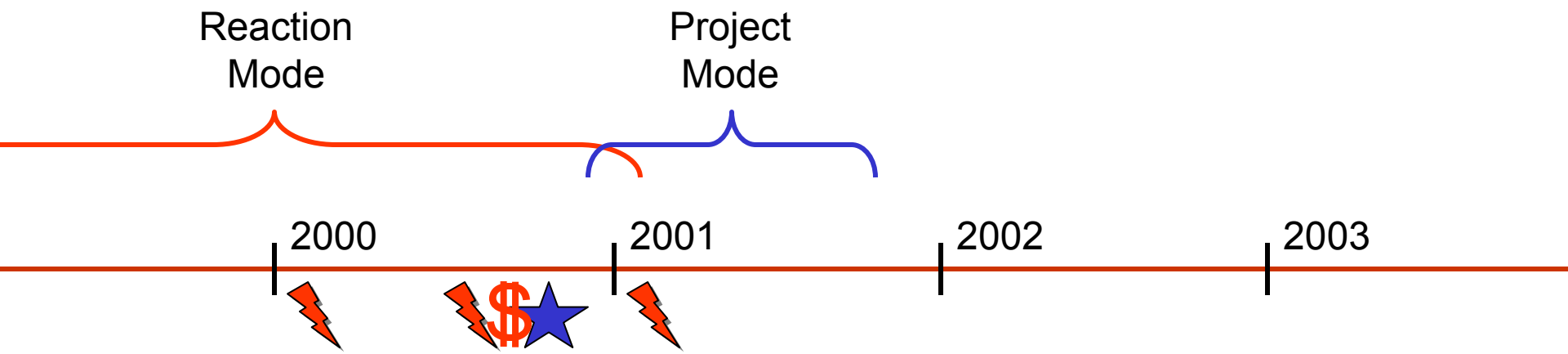
2000 / Reaction

- The scientific community had no desire for strong security.

- General lack of awareness and understanding. At all levels.
- Somebody else's problem.
- No sense of a lab-wide security community.
- Do enough to make the {hackers|auditors} go away.
- Not a process.

- Thus:
  - Lack of funding.
  - No direction.
  - No support.
  - Haphazard implementation.

Moving from Reaction to Intention

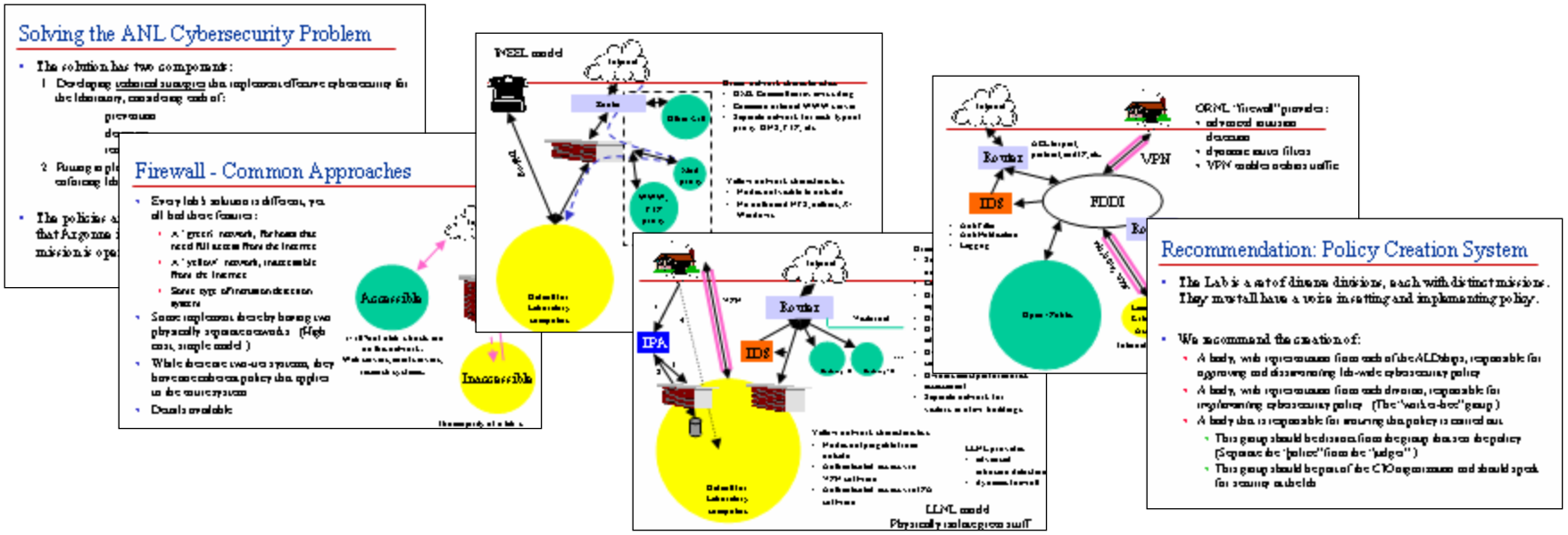


★ New Laboratory Director – first since 1998.

- Management begins to discuss cybersecurity.
- Things start happening…

Internal Briefing

- The Laboratory Director requested an internal report:
  - Confirmed poor security, no plan, no policy.
  - Compared ANL network perimeter to other labs.
  - Recommended the formation of security policy committee.

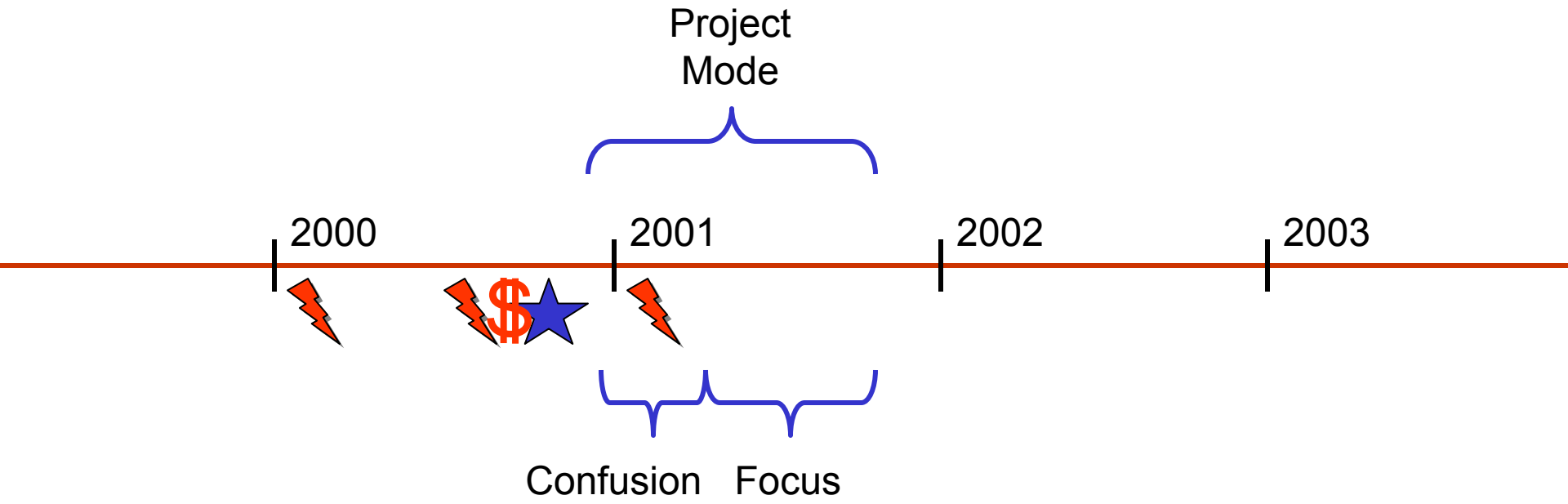


Policies – First Steps

2000 / Project

- The Director formed the Cyber Security Policy Board. (CSPB)
  - Responsible for high-level security policy.
  - Representation from each section of the Lab.
- The CSPB formed the Cyber Security Technical Working Group.
  - Responsible for recommending technical policy to the CSPB.
  - Technical representation from each section of the Lab.
- Immediately started work on:
  - A document stating the Lab's principles.
  - A firewall plan.

Project Mode – Not A Smooth Start



- Unrelated, uncoordinated efforts.
- Plus another audit, which we failed.

- The Deputy to the Lab Director stepped in.
- One project, one goal.

The Goal – Summer 2001

2001 / Project

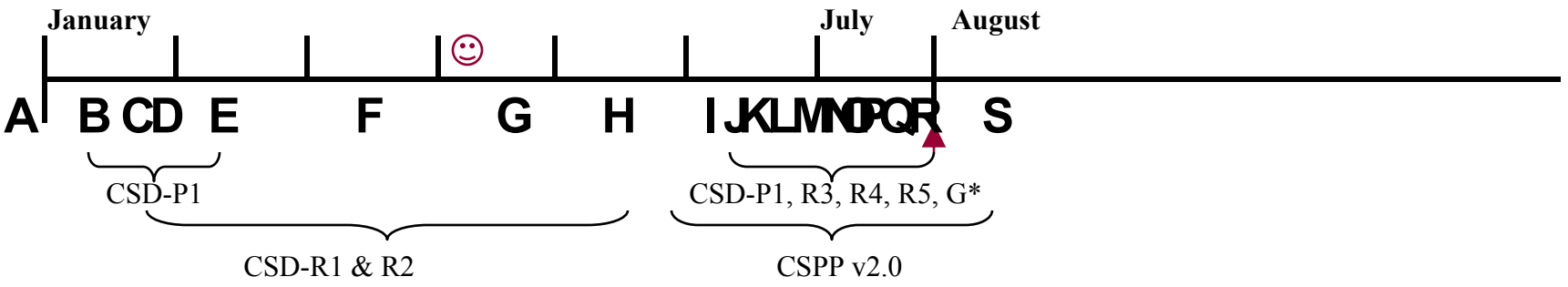
- Fix everything.
- Request an audit before the end of the fiscal year.
- Pass the audit.

- But…
  - Another audit in that time frame was infeasible.

- So…
  - We arranged for a formal peer review.
  - The date was set for August 2001.

Project Calendar – Policy Perspective

2001 / Project

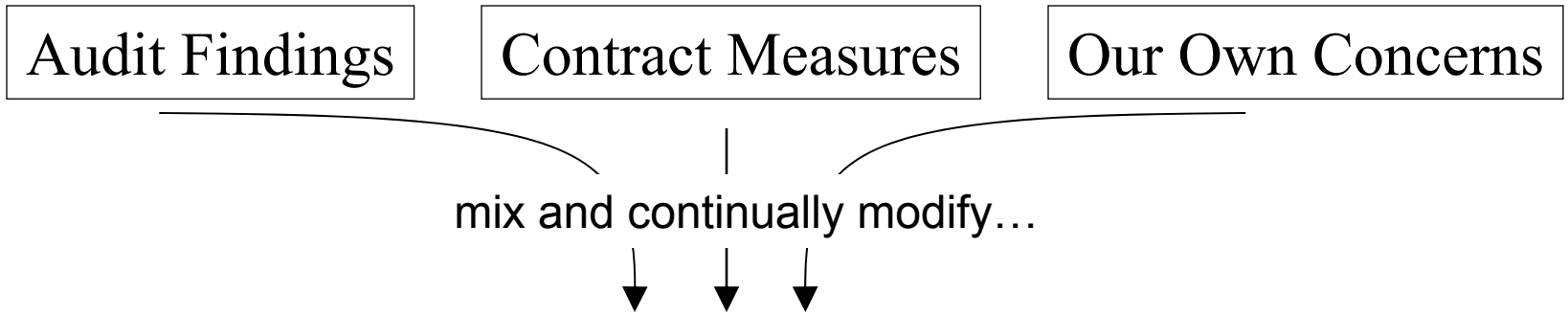


A: Dec 20th – CSPB and CS-TWG formed.
B: Jan 15th – Draft of CSD-P1 released.
C: Jan 24th – Work begins on CSD-R1 & R2.
D: Jan 29th – Public discussion of CSD-P1.
E: Feb 14th – Lab Director approves CSD-P1.
F: Mar 21st – Identify need for CS-ARG.
G: Apr 20th – Draft of CSD-R1 & R2 released, discussion invited and incorporated.
H: May 15th – Comments incorporated into release candidate for R1 and R2.

I: June 5th – July 31st deadline determined.

J: June 12th – CSD-R4 draft.
K: June 18th – CS-ARG formed.
L: June 21st – Password public discussion.
M: June 26th – Remote access public discussion.
N: July 3rd – Banner public discussion
O: July 9th – Drafts of CSD-P2, R1, R3, R4, R5 are up and continually revised based on comments.
P: July 10th – Configuration mgmt discussion.
Q: July 12th – Windows configuration mgmt discussion.
R: July 27th – Technical Checklist released.
S: August 15th – CSPP v2.0 completed, all drafts become policy.

The Components of the Project

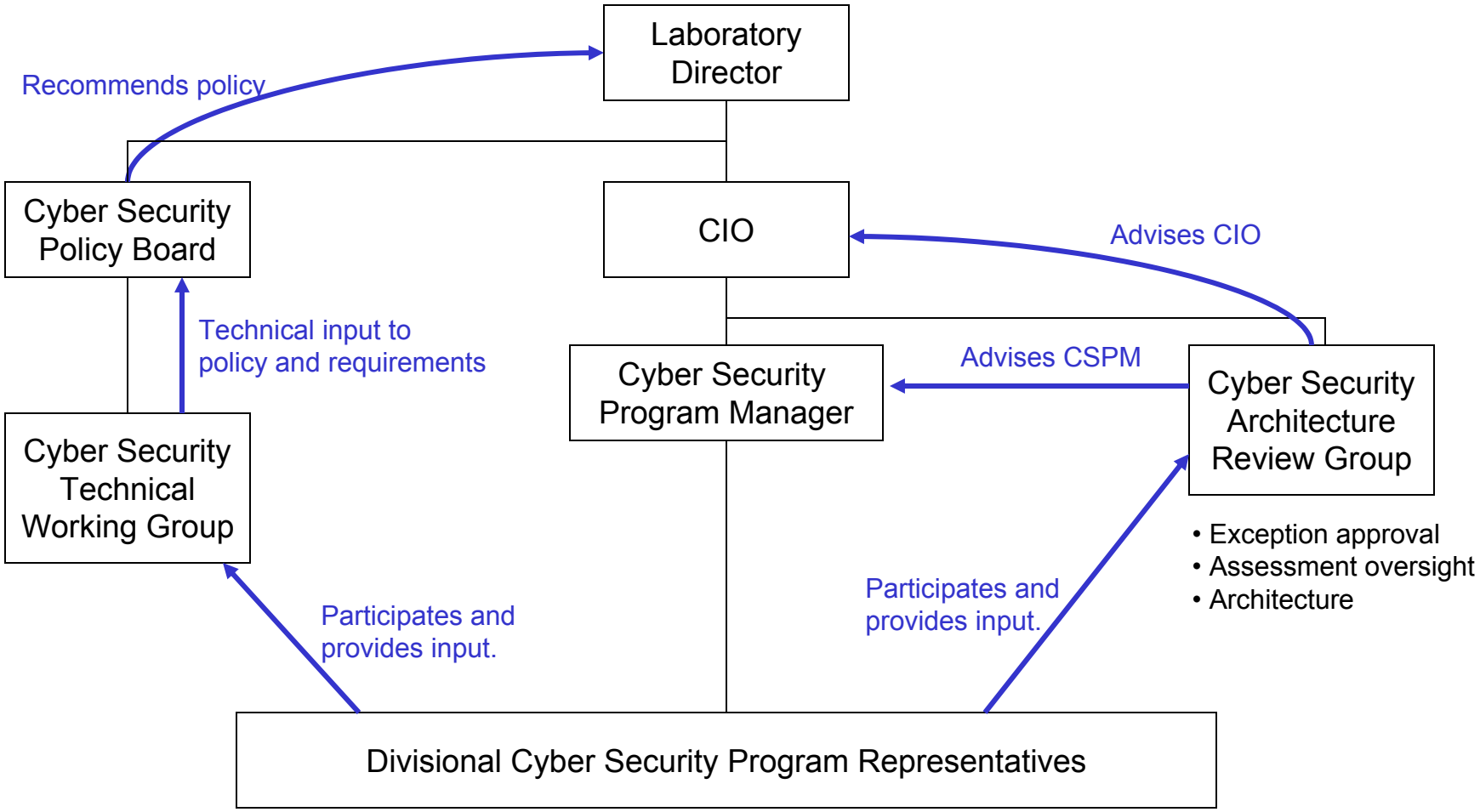


- ★ Responsibility Structure
- ★ Policies and Policy Process
- • Risk Assessments
- ★ Foreign National Access
- • Broad Awareness of Issues
- • Training
- ★ Progress Tracking
- • Technical Reviews

- ★ Network Architecture
  - • Firewalls, VPNs, IDS
  - • Wireless networks
- ★ Host Scanning and Response
- • Host Registration
- • Configuration Management
- • Remote Access
- • Open modems
- • Passwords, banners, …
- • Incident response

Participants in the Policy Process

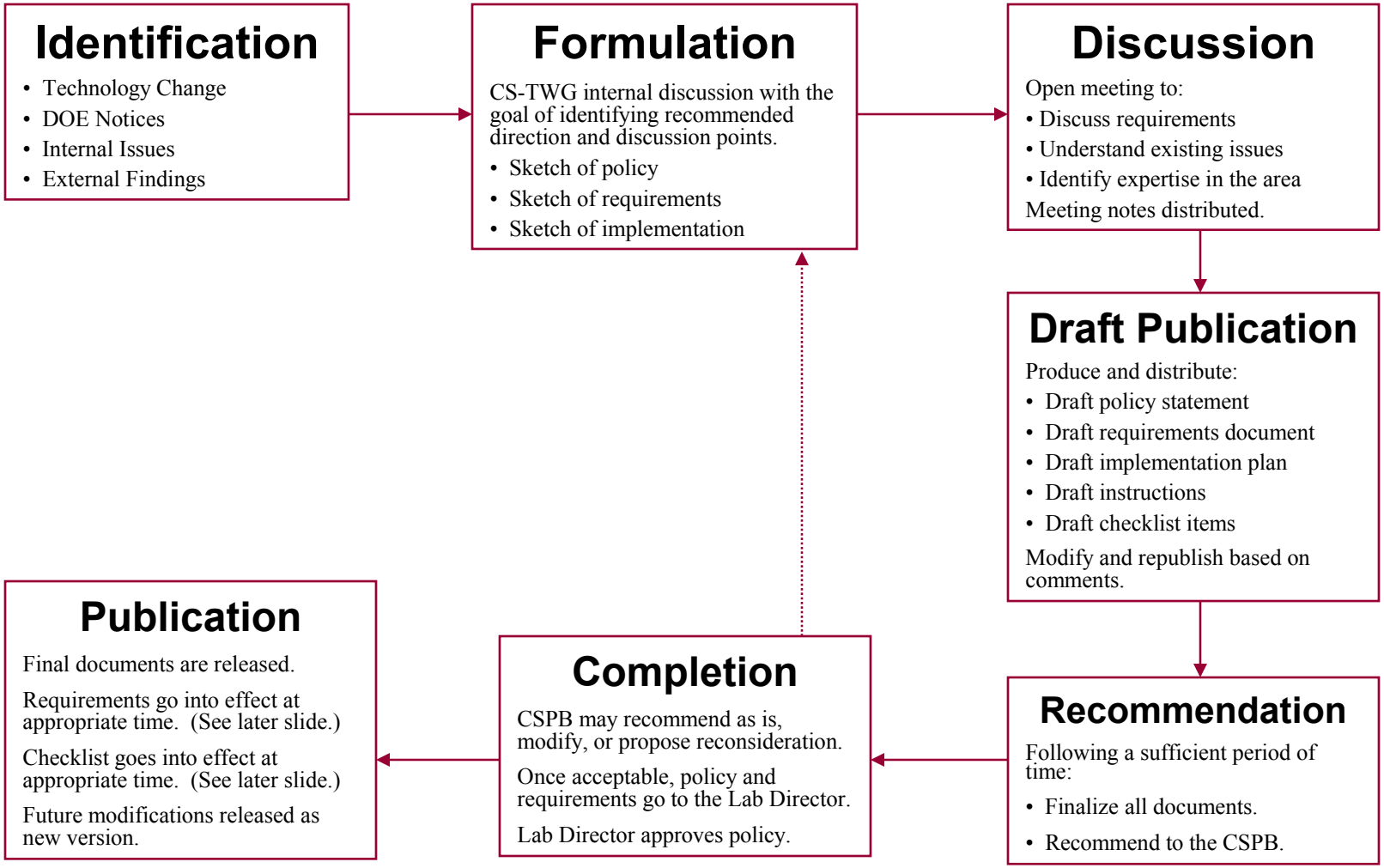
2001 / Project



• Responsible for cyber security implementation in their divisions.

Building Policy

2001 / Project



Policy Description Documents

Policy
(CSPB)

1-2 pages

Technology independent
Establishes principles
Lifespan: 5-10 years

"We will protect our systems from network attacks."

Requirements
(CS-TWG)

10 or so pages

Technology dependent.
Tied to and approved with a policy.
Lifespan: 2-5 years

"We will install firewalls that protect these classes of systems according to these mechanisms…"

General Docs
(CS-TWG)

Variable

Other documents as necessary, such as cookbooks, terminology, configuration checklists.
Lifespan: 2-5 years

"Here's a collection of best practices from around the lab on internal network architecture…"

The CSPP
(CSPM + CSPB + CS-TWG)

The Cyber Security Program Plan is a document required by DOE that gives a broad overview of the program and covers many facets in detail.
It includes all policy and requirements documents, plus additional information.

Codified as the "Cyber Security Document" Series.

For example:
CSD-P1,
CSD-R3,
CSD-G12,
…

Naming convention supports versions. It is described in CSD-G1.

All are available on ANL internal web pages.

2001 CSDs: Policies and Requirements

2001 / Project

Document Number	Title	Contents
CSD-P1	ANL Policy on Cyber Security Fundamental Principles	Cost/risk analysis. Classes of Activities. Roles and Responsibilities
CSD-P2	The Application of Cyber Security Policy	Establishment of CSDs. DOE Notices. Protections. Exceptions.
CSD-R1	Assessments of Class of Activity on ANL Systems	Determining class of activity.
CSD-R2	Network-Based Access to ANL Hosts	Firewalls.
CSD-R3	Password Selection and Management at ANL	Passwords. Education, construction, enforcement. DOE N 205.3.
CSD-R4	Remote Access to and Extension of ANL Networks	Modems. VPNS. External Connections. Remote Access Protocols. Networking Appliances.
CSD-R5	Warning Banners and Public Service Notices at ANL	Warning banners. Notices for public servers.

2001 CSDs: General Documents

2001 / Project

Document Number	Title	Contents
CSD-G1	Overview of the Cyber Security Process	CSD Document Series description Group descriptions Exception mechanisms
CSD-G2	Definitions	Commonly-used definitions
CSD-G4	Password Formation Rules	The exact rules that passwords must meet.
CSD-G5	Password Implementation Guide for UNIX	How to implement the password requirements on UNIX.
CSD-G6	Password Implementation Guide for Windows	How to implement the password requirements on Windows.
CSD-G7	System Administration Practices for UNIX	Recommended best practices for UNIX environments.
CSD-G8	System Administration Practices for UNIX	Recommended best practices for Windows environments.
CSD-G9	System Administration Practices for UNIX	Recommended best practices for Macintosh environments. (Not yet started.)
CSD-G10	Top Priority Fixes for UNIX Systems	Critical security issues that must be addressed on UNIX.
CSD-G11	Top Priority Fixes for Windows Systems	Critical security issues that must be addressed on Windows.
CSD-G12	Top Priority Fixes for Macintosh Systems	Critical security issues that must be addressed on Macintoshes. (Not yet started.)
CSD-G13	Useful Lists for CSPRs	Required documentation, notices for users, etc.

Policy Document Common Themes

- Classes of Data and Activity (defined in CSD-P1)
  - Operations, Proprietary, Scientific, Public, Guest.
  - Varying level of requirements based on class of system.
  - Is a part of the cost/risk analysis.

- Registration Mechanisms (defined in CSD-G1)
  - Certain situations require registration and/or approval.
    - For example: VPNs, Modems, password issues.
  - All such requests go to the CS-ARG.

- Exception Mechanisms (defined in CSD-P2)
  - For exceptions beyond the scope of a standard approval, a division director must submit a request to the CSPB, including a technical assessment from the CS-ARG. The CSPB decision may be appealed to the Laboratory Director.

CSD-R3 – Password Selection and Management (1/3)

- Requirements
  - User Education
    - The Laboratory must create and distribute a guide to secure password selection and handling.
    - Every user must be notified of the password rules at the time of receiving an account on a Laboratory system or gaining access to a Laboratory application that utilizes passwords.
    - All Laboratory computer users must annually be reminded of and acknowledge these password rules.
  - Password Usage
    - All systems that have the ability to make use of passwords in order to access them must do so.
    - All users of all such systems must have passwords.
    - All passwords on all systems must meet the password formation rules as described in CSD-G4.
    - Any passwords generated by a system must meet the password formation rules as described in CSD-G4.
    - Default passwords (e.g. those supplied by vendors) must be changed.
    - Public systems with no passwords must be registered with the CS-ARG.
    - Captive accounts must be registered with the CS-ARG.
    - For systems that employ passphrases in order to access privileged information, such as private keys, those passphrases must meet the password formation requirements in CSD-G4.

CSD-R3 – Password Selection and Management (2/3)

- Requirements
  - Disabling Resources with Insecure Passwords
    - When an account or resource is discovered to have an insecure password, one of the following actions must occur:
      - That account or resource must be deactivated in such a way that the user or an intruder can no longer access that account.
      - The true owner of the account must change the password to a new, secure password.
    - … (many details provided).
  - Password Quality Verification
    - Systems that support multiple users, allow network-based access to resources, and have lists of passwords that are readily accessible to the administrators of the system must be checked regularly for insecure passwords.
      - Systems that do not enforce strong passwords through some automatic mechanism must have their passwords quality-checked every 3 months.
      - Systems that enforce strong passwords through some automatic mechanism must have their passwords quality-checked every 6 months.

CSD-R3 – Password Selection and Management (3/3)

- Requirements
  - Password Management
    - Systems must meet as many of the following requirements as possible:
      - The system must allow the entry of passwords per CSD-G4.
      - If passwords are generated for users of the system by some process, that process must generate passwords per CSD-G4.
      - The system must enforce the selection of passwords per CSD-G4.
      - The system must require users to change their passwords at least every six months.
      - The system must detect three failed attempts to provide a password and lock out subsequent attempts until some reasonable amount of time (as decided by the system manager, as part of a risk analysis) has passed.
      - Any list of passwords (e.g., /etc/passwd) must be protected from access by unauthorized individuals.
    - Some Laboratory systems that employ passwords cannot meet all of these requirements because of technical or functional limitations. All network-accessible systems and applications that do not meet these requirements for passwords must be registered with the CS-ARG.
  - Clear-Text Passwords
    - Not allowed except under very limited circumstances. The Laboratory will block clear-text protocols between divisions and at the border.

Policy Implementation Documents

2001 / Project

Instructions
(CS-TWG)

A web page.

Tied directly to a requirements document.

"1. Get behind firewall."
"2. Register necessary conduits.
…"

Checklist
(CS-TWG)

A portion of a web page.

Tied directly to an instructions document.

"1. Are you behind the firewall?."
2. Have you registered the necessary conduits?
…"

Implementation Plans
(Responsible Party)

Project documents.

When infrastructure is necessary for requirements, project plans are created.

"We will purchase a LX-16j firewall for $42K and install it in March 2001…"

The Technical Checklist
(CSPM + CS-TWG)

The Technical Checklist is a web-based tracking system for all requirements. Every division records their status on the checklist. This is used as a Lab metric.

Technical Checklist – Progress Tracking

- The Technical Checklist is a web application at:
  - http://www.mcs.anl.gov/cybersecurity/checklist/cs-progress.php
  - Used in an on-going fashion.
  - Each CSPR updates their own checklist as they make progress.
  - Current summary always available:

Division	Total	Class Assessment	Banners	Configuration	Firewall	Passwords	Remote Access	Risk Assessment
ANL-W	36 / 53 67%	0 / 4 0%	7 / 7 100%	0 / 2 0%	3 / 3 100%	13 / 16 81%	12 / 17 70%	1 / 4 25%
APS	48 / 53 90%	4 / 4 100%	7 / 7 100%	2 / 2 100%	3 / 3 100%	13 / 16 81%	15 / 17 88%	4 / 4 100%
BIO	48 / 53 90%	4 / 4 100%	7 / 7 100%	0 / 2 0%	3 / 3 100%	13 / 16 81%	17 / 17 100%	4 / 4 100%
CHM	50 / 53 94%	4 / 4 100%	7 / 7 100%	2 / 2 100%	3 / 3 100%	15 / 16 93%	15 / 17 88%	4 / 4 100%
CIP	53 / 53 100%	4 / 4 100%	7 / 7 100%	2 / 2 100%	3 / 3 100%	16 / 16 100%	17 / 17 100%	4 / 4 100%
CMT	52 / 53 98%	4 / 4 100%	7 / 7 100%	2 / 2 100%	3 / 3 100%	15 / 16 93%	17 / 17 100%	4 / 4 100%
DEP	49 / 53 92%	4 / 4 100%	7 / 7 100%	1 / 2 50%	3 / 3 100%	16 / 16 100%	14 / 17 82%	4 / 4 100%

Additional Process and Cultural Activities

2001 / Project

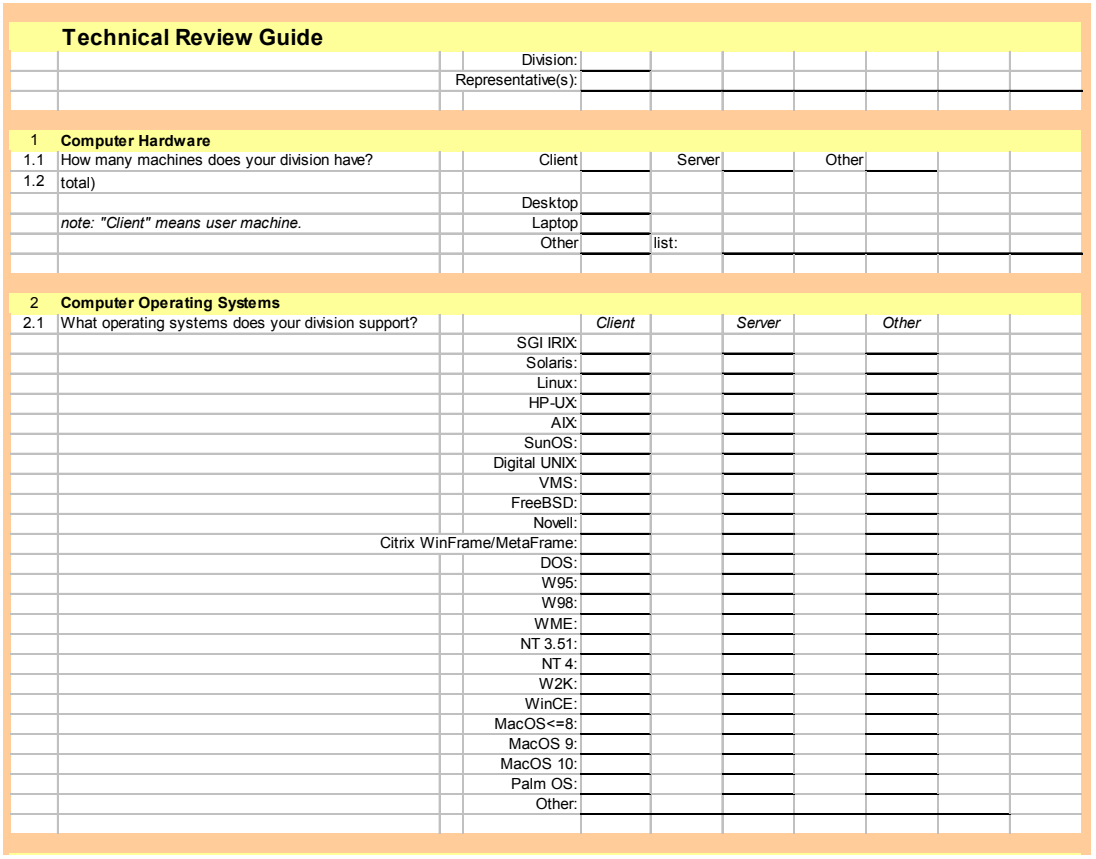
- Risk Assessments
  - Every division followed forms for carrying out detailed risk assessments.
  - We identified a number of "critical assets" that needed special assessments.
- Foreign National Access
  - DOE requires special handling of accounts for foreign nationals.
  - We clarified the requirements and everyone confirmed they met them.
- Broad Awareness
  - Password cubes. Posters. High-visibility talks.
  - Memos and updates to division directors.
  - ★ "All-Hands" risk assessment meeting.
- Training
  - Training of everyone on passwords and basic security.
  - SANS courses for sysadmins.
  - Tracking mechanisms.

★ Technical Reviews
  - The CS-ARG visited every division on site.
  - The goal: understand what was out there. Understand the issues. Raise awareness.

Technical Review Guide

2001 / Project

- One of the Risk Analysis workbooks.
- Each division fills this out.
- Covers:
  - Hardware
  - Enclaves
  - Network
  - Remote Access
  - Systems Team
  - Users
  - Security Incidents
  - Configuration
  - Host Database
  - Physical Security
  - Development
  - Management



Technical Review Guide

Division:
Representative(s):

1 **Computer Hardware**

1.1 How many machines does your division have? Client Server Other
1.2 total)
Desktop
note: "Client" means user machine. Laptop
Other list:

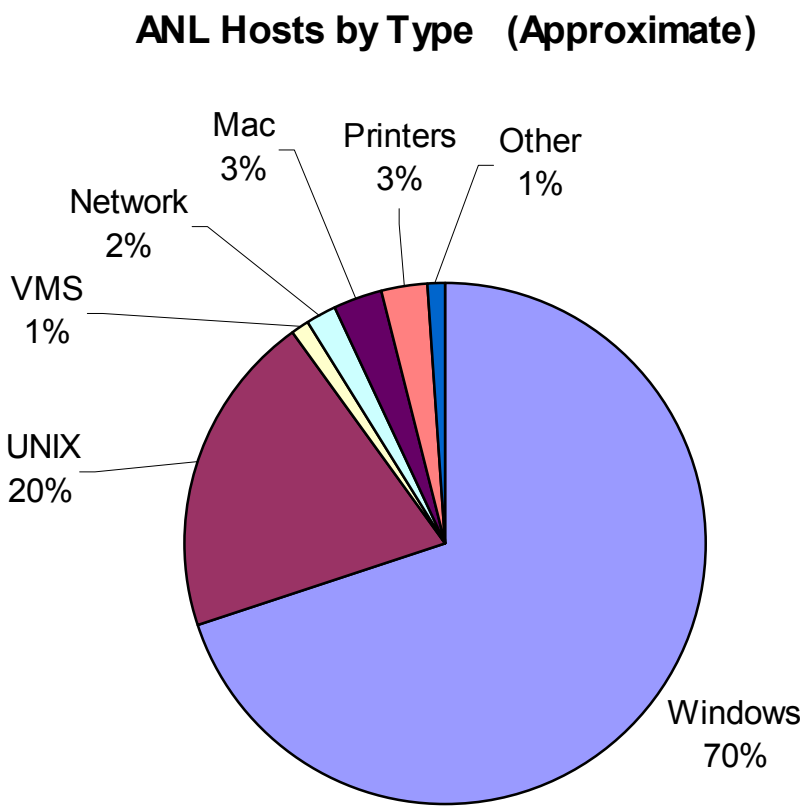
2 **Computer Operating Systems**

2.1 What operating systems does your division support?

	Client	*Server*	*Other*
SGI IRIX:			
Solaris:			
Linux:			
HP-UX:			
AIX:			
SunOS:			
Digital UNIX:			
VMS:			
FreeBSD:			
Novell:			
Citrix WinFrame/MetaFrame:			
DOS:			
W95:			
W98:			
WME:			
NT 3.51:			
NT 4:			
W2K:			
WinCE:			
MacOS<=8:			
MacOS 9:			
MacOS 10:			
Palm OS:			
Other:			

Laboratory Hosts

2001 / Project



Approximately 8500 total systems.

Laboratory Scanning

2001 / Project

- Laboratory scanning was actually started in 2000 as part of the early risk assessment process.
  - This is trickier than one might think.

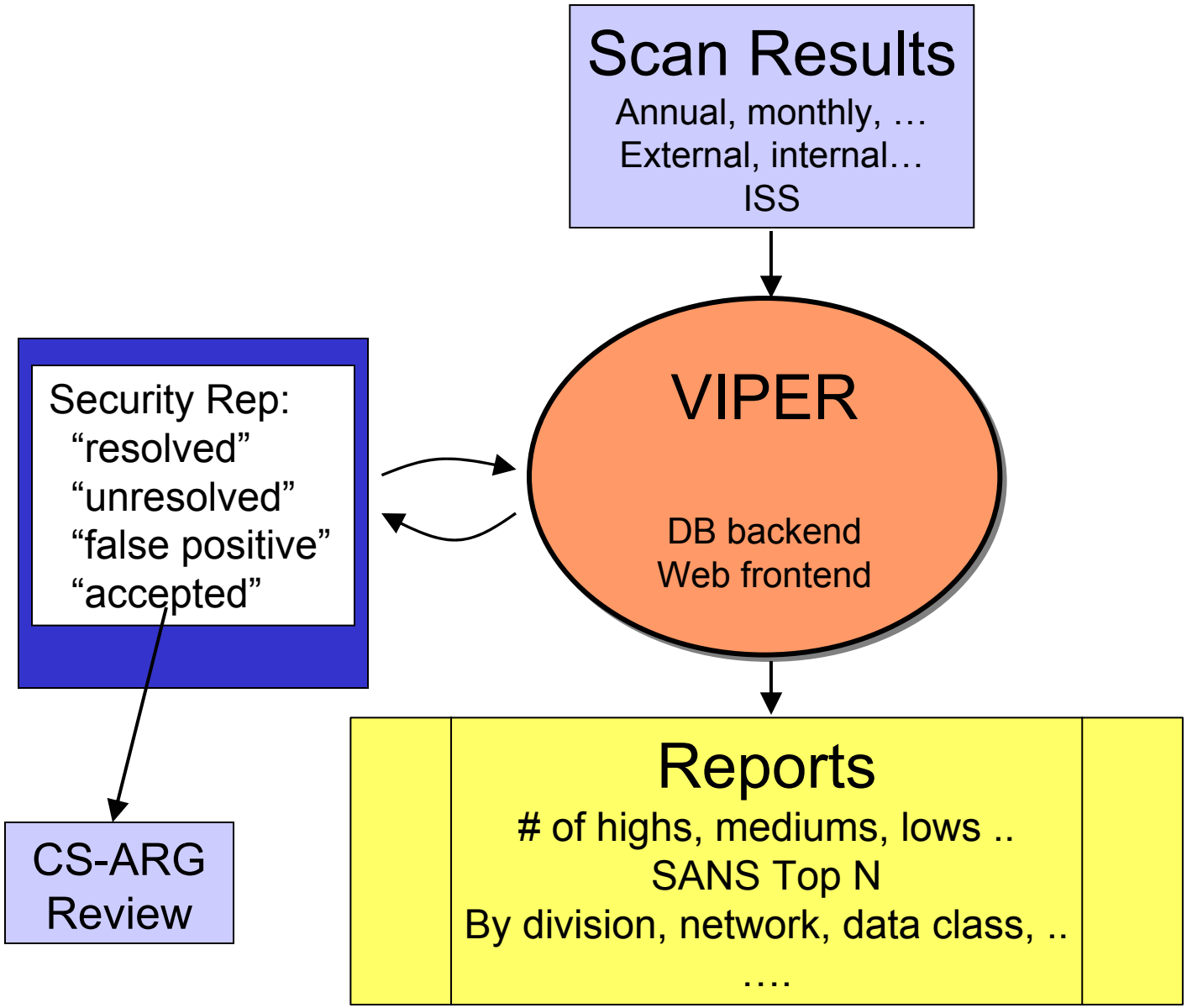
- Progress:
  - 25% of all networks complete by May 30
  - 100% complete by July 13

- Findings:
  - 3462 high.
  - 9524 medium.
  - Many of these are false positives.

- Goals:
  - Highs corrected by Sep. 10th.
  - Mediums corrected by Nov. 5th.

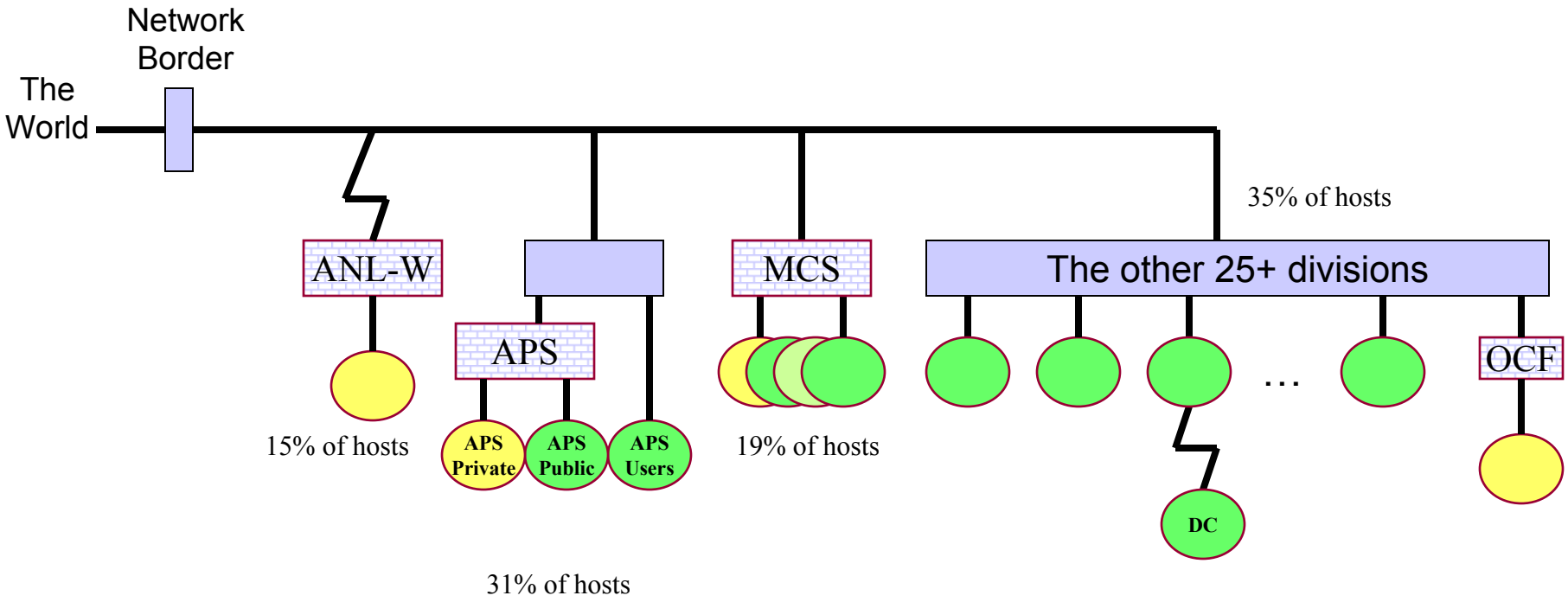
VIPER – Tracking Scans

2001 / Project



Network: Pre-Firewall

2001 / Project



Hosts, mostly protected

Hosts, mostly unprotected

Networks and network gear

Network protection

WAN

The Firewall – A Divisive Challenge

2001 / Project

Firewalls are evil…

If it's not stateful, it's not a firewall.

The Lab should only have one firewall,

Oh, and one web server, one ssh server, one mail server, …

I don't have the cycles to cope with this change.

Green networks. Yellow networks.

I have my own firewall, leave me alone…

2 or more separate physical networks…

DOE requires this. DOE requires that.

Firewalls are too expensive…

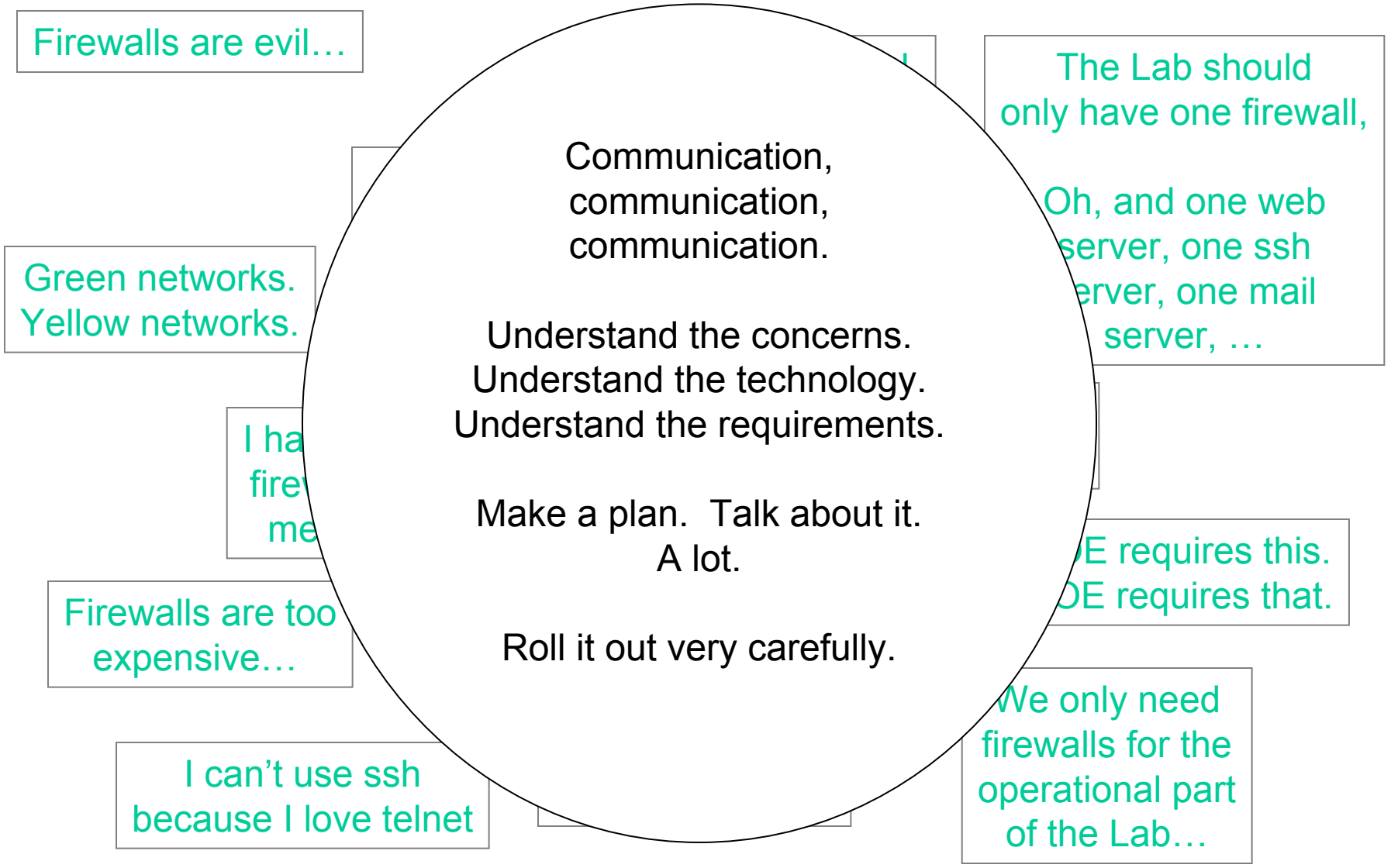
I'm afraid that someone else's firewall will break my network.

We only need firewalls for the operational part of the Lab…

I can't use ssh because I love telnet

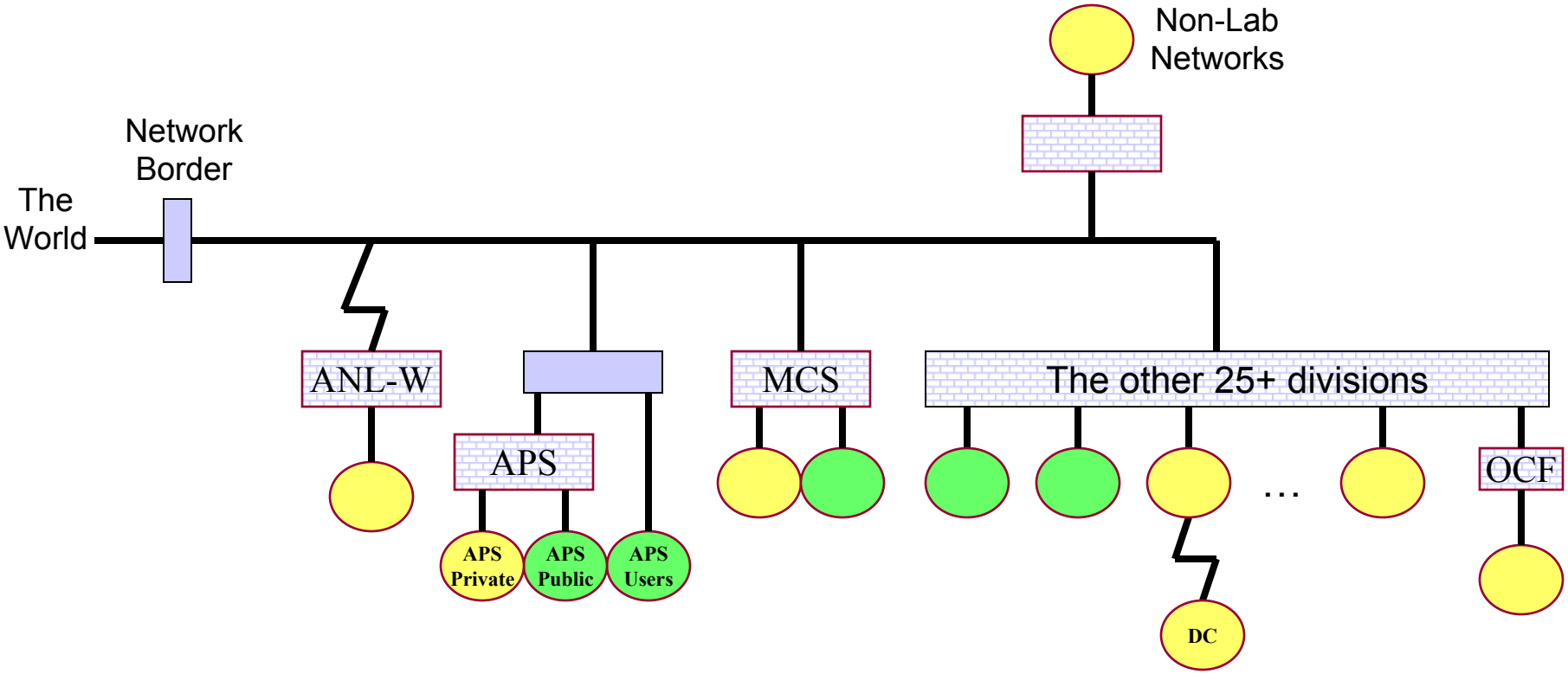
The Firewall – A Divisive Challenge

2001 / Project



Network: Firewall Transition

2001 / Project

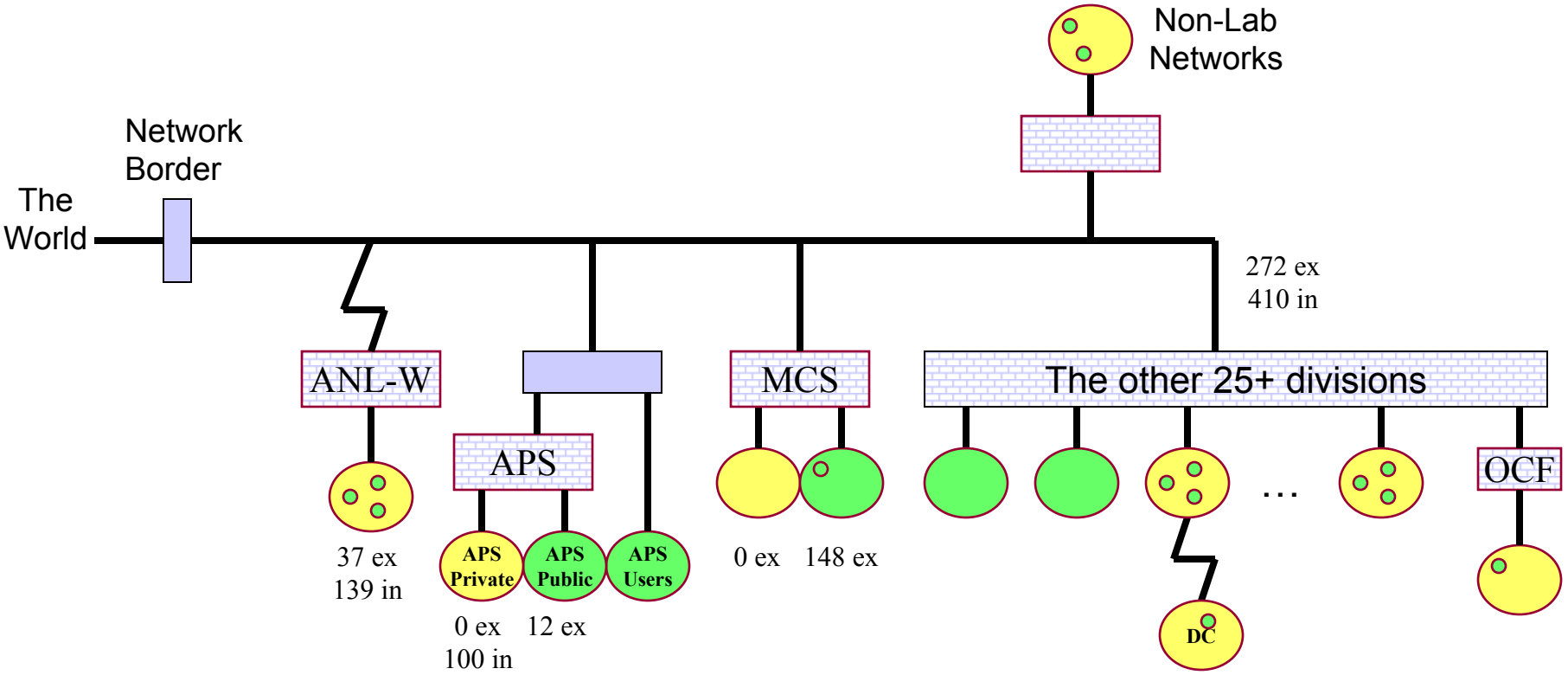


- Firewall testing for months.
- Ran it in passive mode.
- Ran netflow analyses.
- Asked security reps which traffic should be allowed.
- Sanity checking.

- In July 2001:
  - The firewall was deployed.
  - All networks were shifted to it.
- Very few problems.

Network: Yellow With Green Dots

2001 / Project



- We had to support existing traffic.
- Most “yellow” networks had hosts with conduits through their firewall.
- “ex” = conduit for external IP(s), “in” = conduit for internal IP(s).

Network: Firewall Coordination

- All firewalls are operated in synchrony.
  - Meetings of the firewall personnel.
  - Mailing lists for discussion, alarms, and policy notifications.
  - Pager/Phone information coordinated.
  - MOU in place defining the agreement.

- Laboratory Firewall policy applies to all firewalls.

Registration and Approvals

- Forms for all types of registration and approvals are on the web.
  - Criteria for meeting approvals are also on the web.

Req #	Age	Status	User	Subject
50	14 hr	open	dick.eagan	Password Shortcomings by Ma
49	2 day	open	dseymour@a	WWW request
48	2 day	open	vberardi@a	Password deviations from CS
47	2 day	open	vberardi@a	INBOUND MODEM REGISTRATION
46	2 day	open	evard@mcs.	general exception for DEP
45	2 day	open	mskwarek@a	Password 205.3 - Windows Sy
44	2 day	open	cbeles@dep	Request for Exception
43	3 day	open	mattk@anl.	Web Cam Server Firewall Req
42	3 day	resolve	dseymour@a	Dial-In Modem Registration
41	5 day	resolve	tehren.kil	Amended Firewall access req
40	4 day	open	osudar@cmt	Complex Firewall: CMT secu
39	4 day	open	osudar@cmt	Complex Firewall: CMT SSH s
38	4 day	open	osudar@cmt	Complex Firewall: CMT Wind
37	4 day	resolve	osudar@cmt	CMT Dial-Out Modems
36	4 day	open	mcharan@an	Fwd: FW: open port request

- Requests
  - come in via email
  - are processed via a ticket system
  - will be archived in a database
- The CS-ARG meets regularly to process requests.
- “Standard” firewall requests, if they pass a scan and meet criteria, can be handled immediately.

CS-ARG Firewall Conduit Criteria for UNIX hosts

2001 / Project

1. The system is configured at current vendor recommended security patch level.
2. The system is configured to address all relevant CIAC recommendations.
3. There is a procedure in place to ensure that system configuration is kept current with respect to patches and CIAC notices.
4. All un-necessary system services disabled per CSG-G7, #10.
5. All running system services configured in a secure manner.
6. The system passes Laboratory Standard network vulnerability scans (using ISS as of this writing).
7. System passes workstation vulnerability scan using a tool such as CIS.
8. A host-based intrusion detection system (for example, tripwire or aide) is installed and run at least each workday,
9. The system implements the ANL banner policy per CSD-R5.
10. The system implements the ANL password policy per CSD-R3.
11. The system has an assigned system administrator with greater than 2 years experience with UNIX systems security.
12. If the request is for off-site access to a service:
    - Only related off-site services are allowed to run on the system, and all such services must be listed in the exception request.
    - The system has no 'trust' relationships or dependencies on other ANL systems.
    - System is physically secure.
    - The system is configured as a server with no 'general use' users.
    - The system access logs are maintained and reviewed at least each workday.

Additional Technical Activities

2001 / Project

- Network Perimeter and Architecture
  - The Laboratory Firewall
  - Intrusion Detection System
  - VPN deployment
- Lab Scanning
- Tackled Wireless Networks
  - Had to be registered. Had to meet some minimum criteria.
- Host Registration
  - All hosts needed to be registered in a central database, along with their “class”.
- Configuration Management
  - Issued a series of best practice documents.
  - Hosts with conduits had to meet those as requirements.
- Open Modems
  - Carried out extensive war dialing.
  - All modems allowing dial-in had to be registered.
- Incident Response
  - The CS Office and the CS-ARG acted as a response team.

The 2001 Peer Review

- August 20-22, 2001

- Peer Review Membership
  - Ian Bird, Thomas Jefferson National Accelerator Facility
  - Robert Cowles, Stanford Linear Accelerator Center
  - Dave Grubb, Lawrence Livermore National Laboratory
  - Gregory A. Jackson, The University of Chicago (chair)
  - Matt Crawford, Fermi National Accelerator Laboratory
  - Robert Mahan, Pacific Northwest National Laboratory
  - Walter Dykas, Oak Ridge National Laboratory
  - James Rothfuss, Lawrence Berkeley National Laboratory

- Process
  - Presentations on cyber security and IT.
  - Formal and informal interviews with staff.
  - “All discussions were spirited and frank.”

Institutional Change

2001 / Project

This effort has redefined Cyber Security at ANL. It is well on track to meet all goals and address all findings by the end of the FY. The Laboratory is far more secure than it ever has been.

But have we built the foundation for the necessary institutional change?

"No":

- This all took place too quickly.
  - Institutional change cannot take place that quickly or be assessed on such a short time frame.
- This only happened in response to audits and deadlines.
- Is the structure in place sufficient to survive personnel changes?
- Can the Lab respond to the results of the General Lab-Wide Risk Assessment?

This question was posed to the peer review committee of 2001.

"Yes":

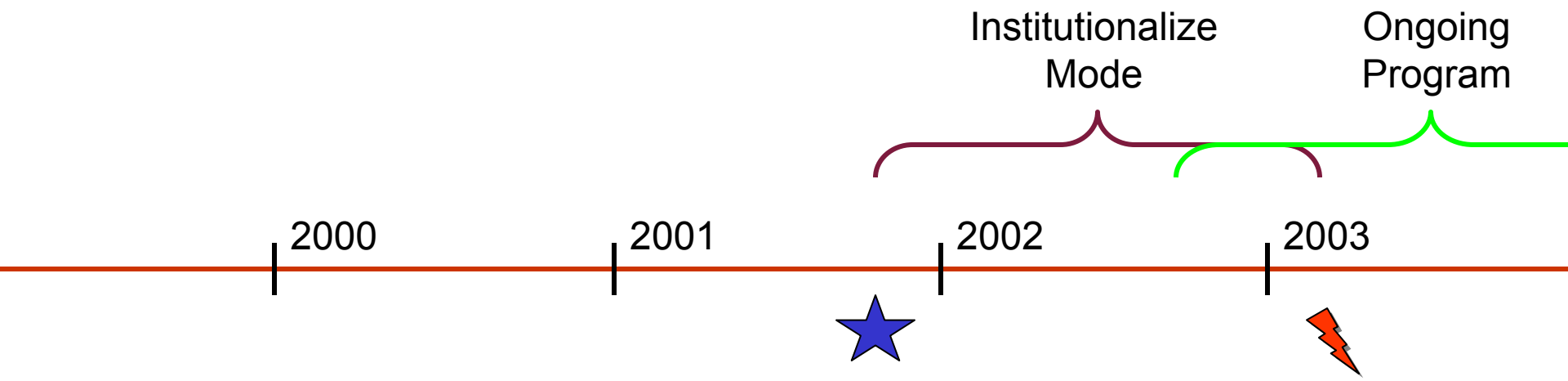
- Change starts with comprehension. We're seeing evidence of understanding, e.g.:
  - Division directors are very aware of these issues and are asking what they can do.
  - Internal reviews indicate a more broad awareness of the topics.
- Broad lab-wide involvement.
  - No one is thrilled about spending the extra time. Everyone notes that it must be done.
  - Amazing amount of effort. You don't do that if you think the problem will "go away".
- Real plans are in place for all aspects of this project through 2002.
- Strong management support.

Peer Review Findings

2001 / Project

- Central Observations
  - “In our experience it is rare to find the degree of high-level support combined with grass-roots collaboration we observed at ANL. This kind of commitment is central to effective cyber-security.”
  - “We find the rate of progress in ANL’s cyber-security efforts laudable and impressive, especially given the late start and scattered success on which it is based. In our view, the rate of cyber-security progress at ANL is exemplary among its peers.”
  - “ANL’s rapid progress is leading toward a very high level of cyber-security, one that, when attained, should place it high among its peers.”
- Many positive comments.
- Recommendations
  - Simplify the risk-assessments.
  - Focus on goals.
  - Worry about some of the technical directions (NAT, single-sign-on, others).
  - Worry about steady-state management.
  - Can the project transform itself into a program?

Institutionalizing the Project



- The goals:
  - Reduce the effort level – but sustain the energy.
  - Clean up.
  - Be prepared for the next audit.
  - Make cybersecurity a part of the Lab's culture.

- The primary activities:
  - Organization and process.
  - Network and security architecture.

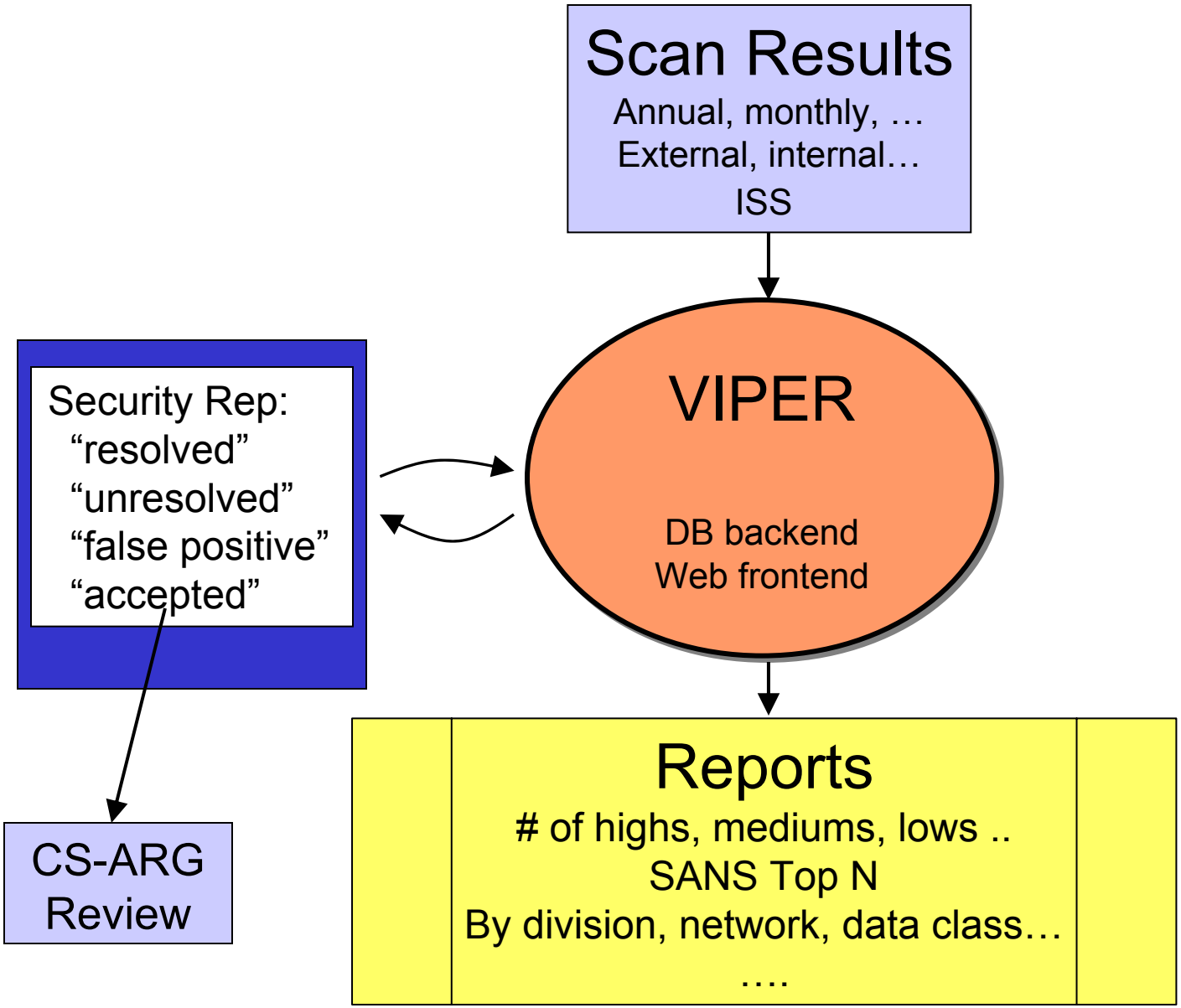
Technical Activities

2002 / Institutionalize

- Lab Scanning
  - Improvements
- Network Perimeter and Architecture
  - Cleaning up
  - Improvements
  - Rethinking wireless.
- Host Registration
  - Decided the central database wasn't working.
  - Shifted to coordinated, decentralized db.
- Configuration Management
  - Refined the best practice documents.
  - Created centralized resources – e.g. validated distros.
  - Did **not**: create new requirements or increase centralization.
- Foreign Nationals
  - Created a web-based registration and review process.
- Registration Integration
  - Web-based forms for registration and conduit requests
  - IP address is automatically checked for proper "color" vs. service being requested (ANL only vs. Internet access)
  - Automatically schedules a scan of the IP address
  - Conduit automatically removed if med/high vulnerabilities are found on the hosts

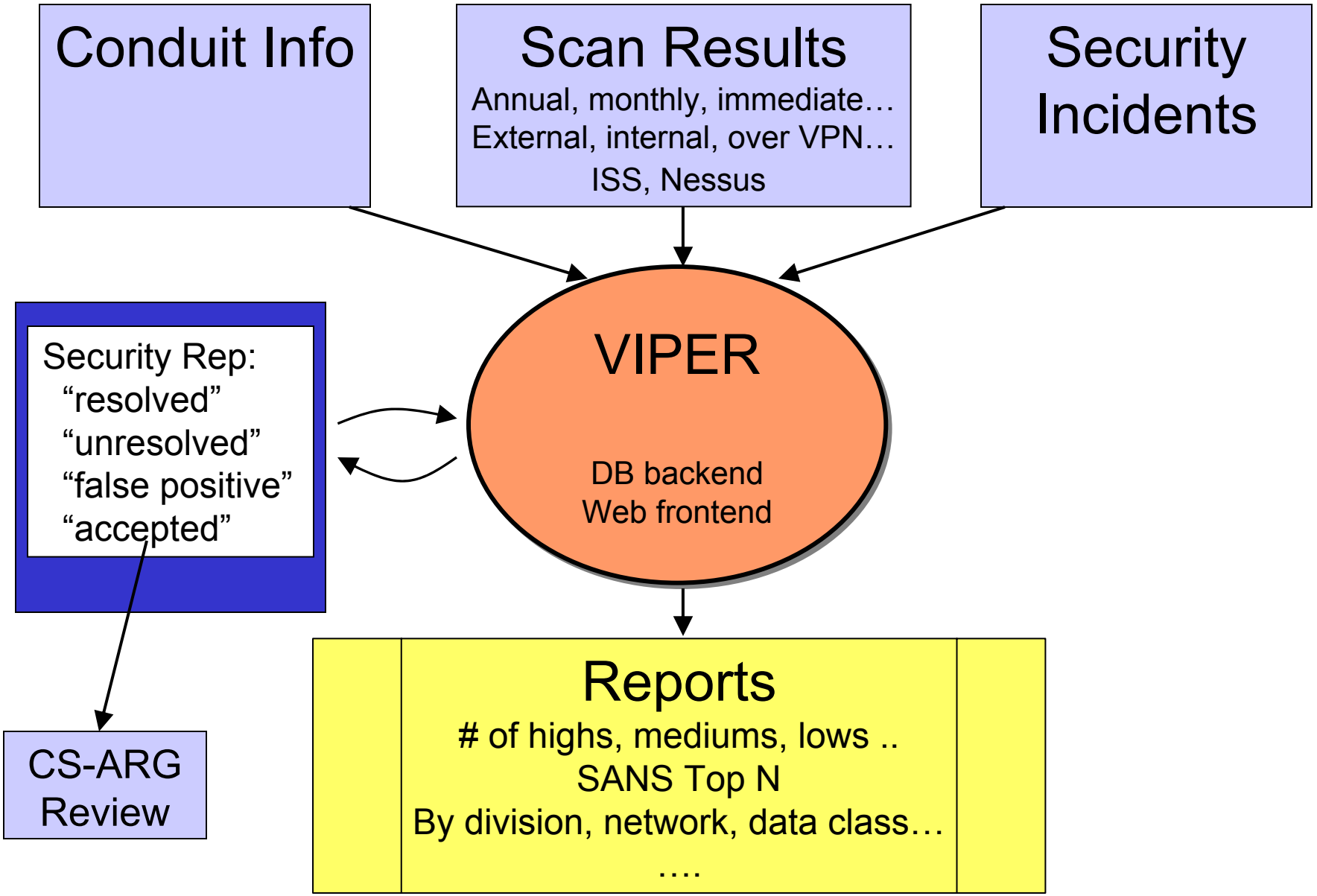
Overall:
More consistency.
Better integration.
Practical solutions.

VIPER – Tracking Scans



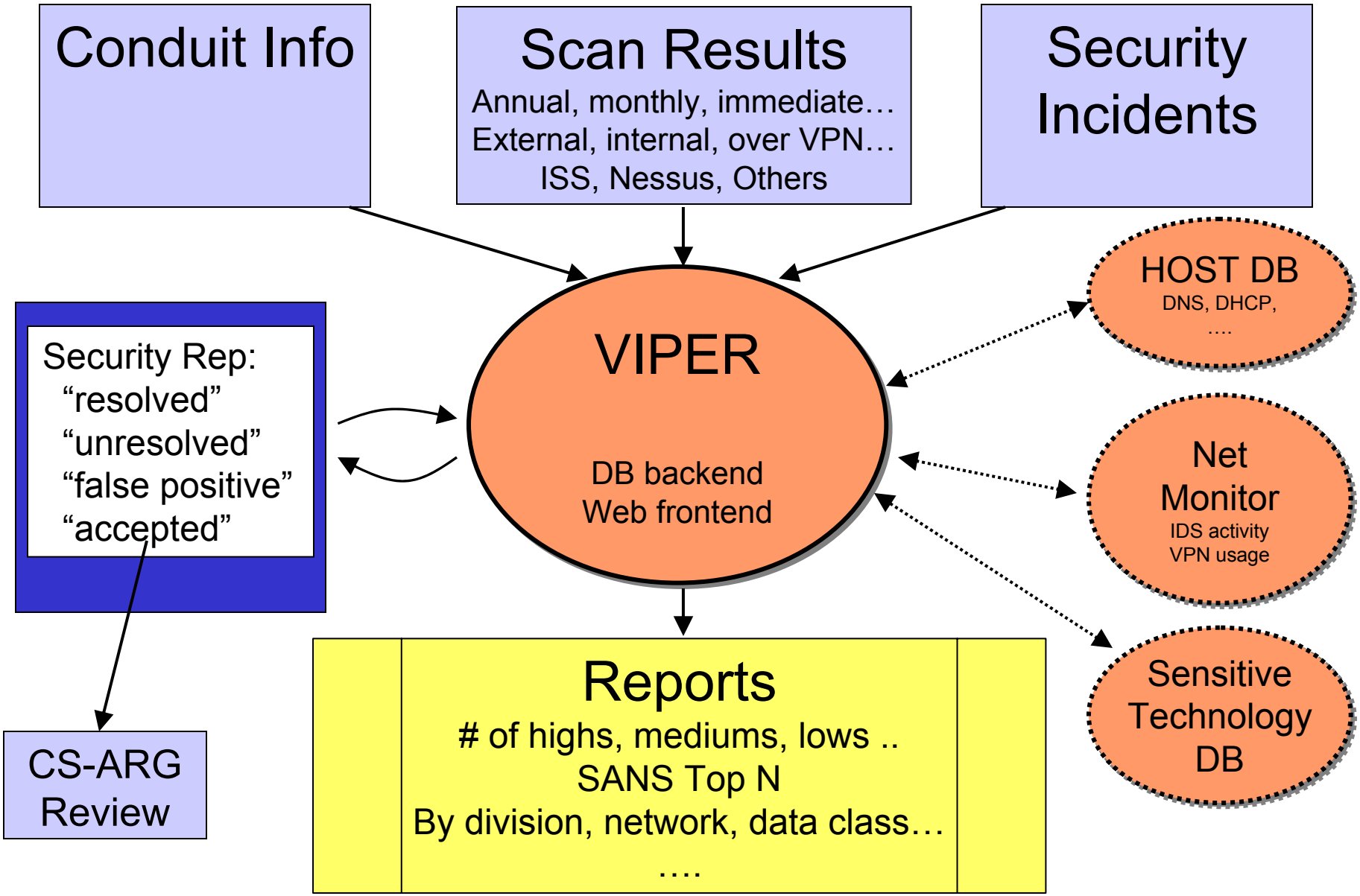
VIPER – Institutionalization

2002 / Institutionalize



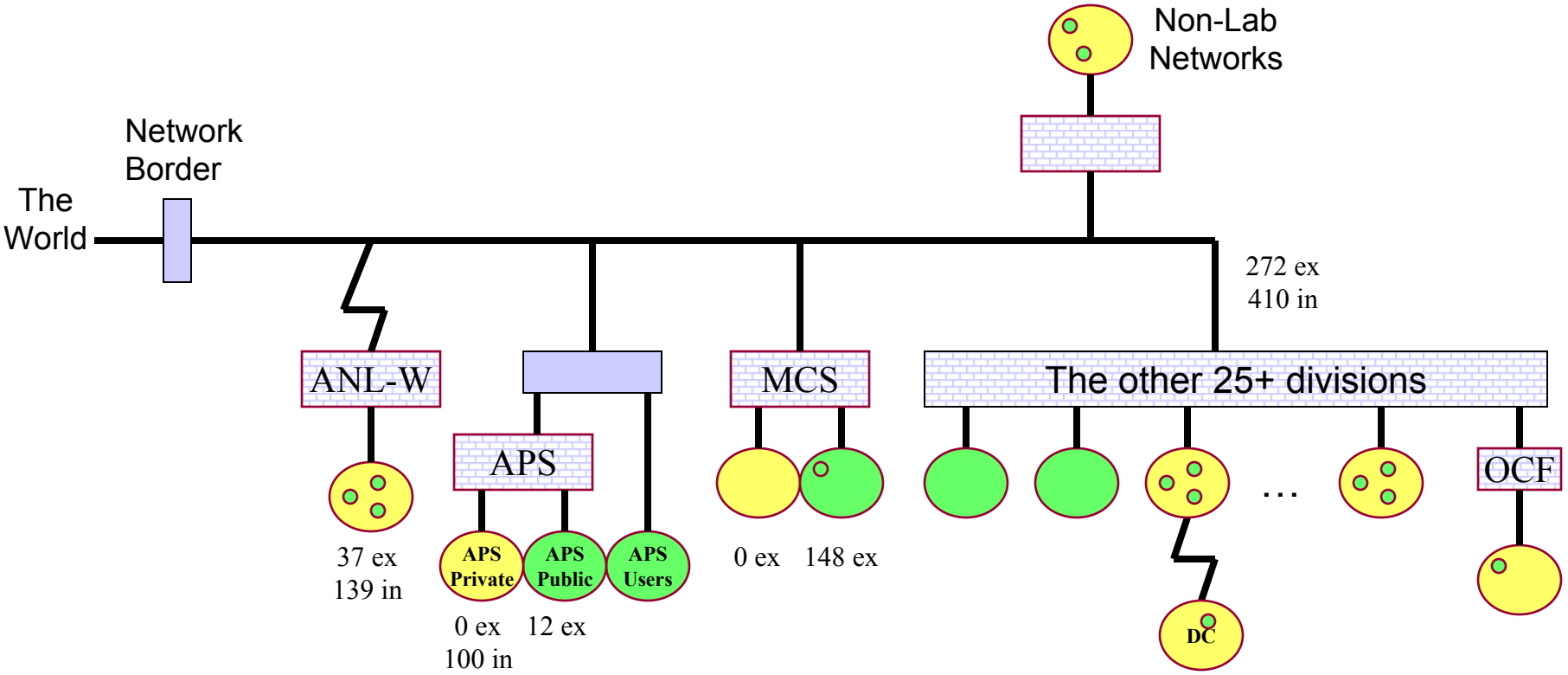
VIPER – Futures

2003 / Program



Network: Yellow With Green Dots

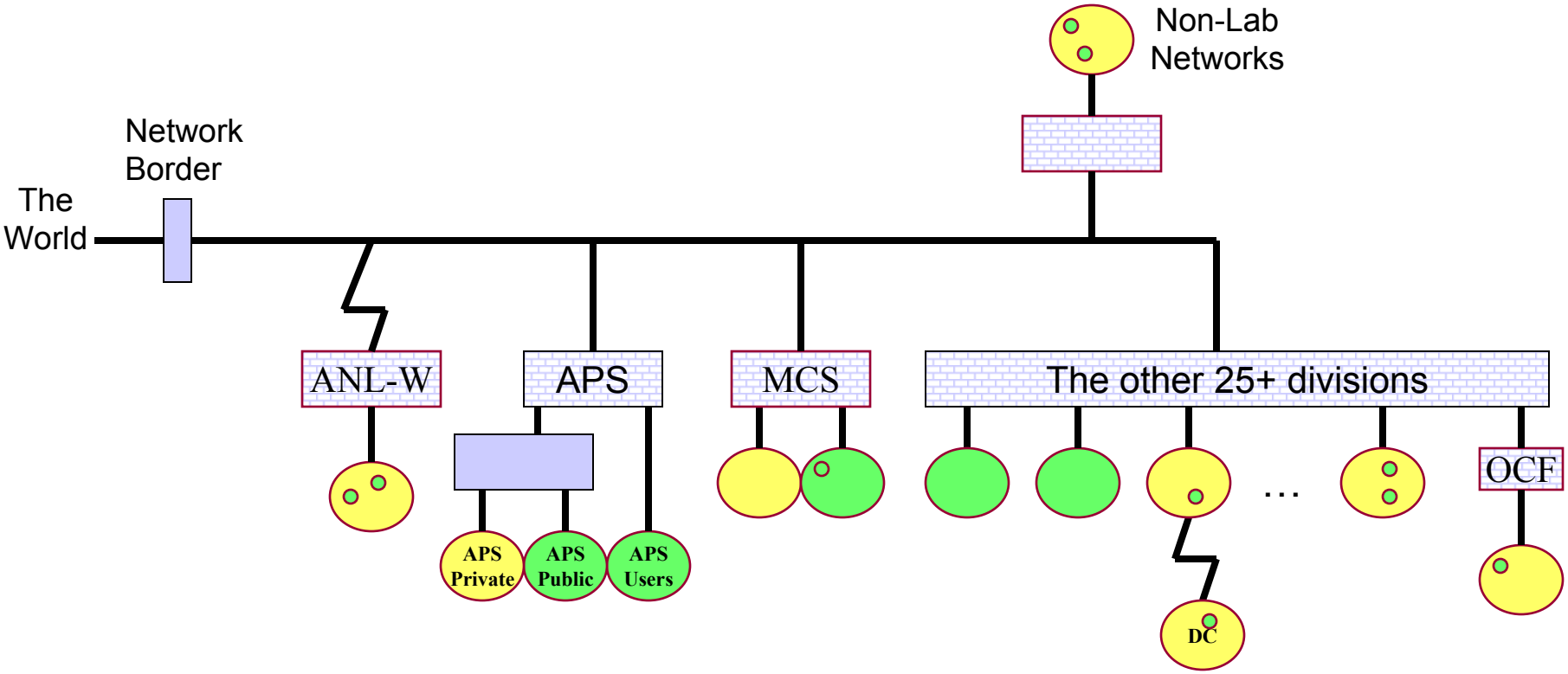
2001 / Project



- We had to support existing traffic.
- Most “yellow” networks had hosts with conduits through their firewall.
- “ex” = conduit for external IP(s), “in” = conduit for internal IP(s).

Network: The Conduit Crunch

2002 / Institutionalize



- Any new conduits had to be approved.
- All existing conduits had to be approved.
- At completion: down to ~200 conduits

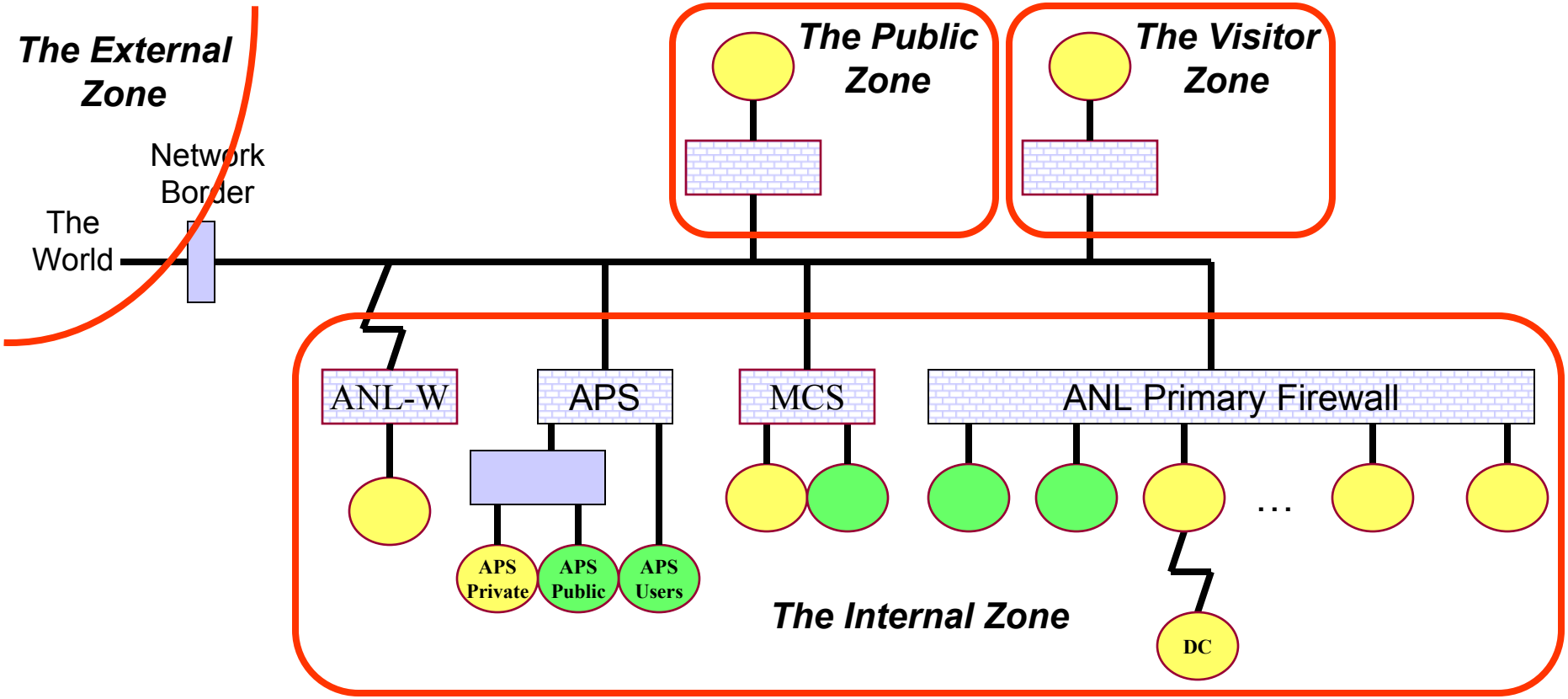
- Oct: FTP, POP, Telnet, Any
- Dec: VNC, PC Anywhere, Netbios
- Feb: DNS, Anon FTP, SSH, and zero-hit conduits
- Mar: All remaining.

Network: Concerns

- Security representatives were confused.
  - Yellow, yes. Green, ok. Yellow with green dots?
- No protection against internal threats.
- No containment.

Network: Zone Architecture

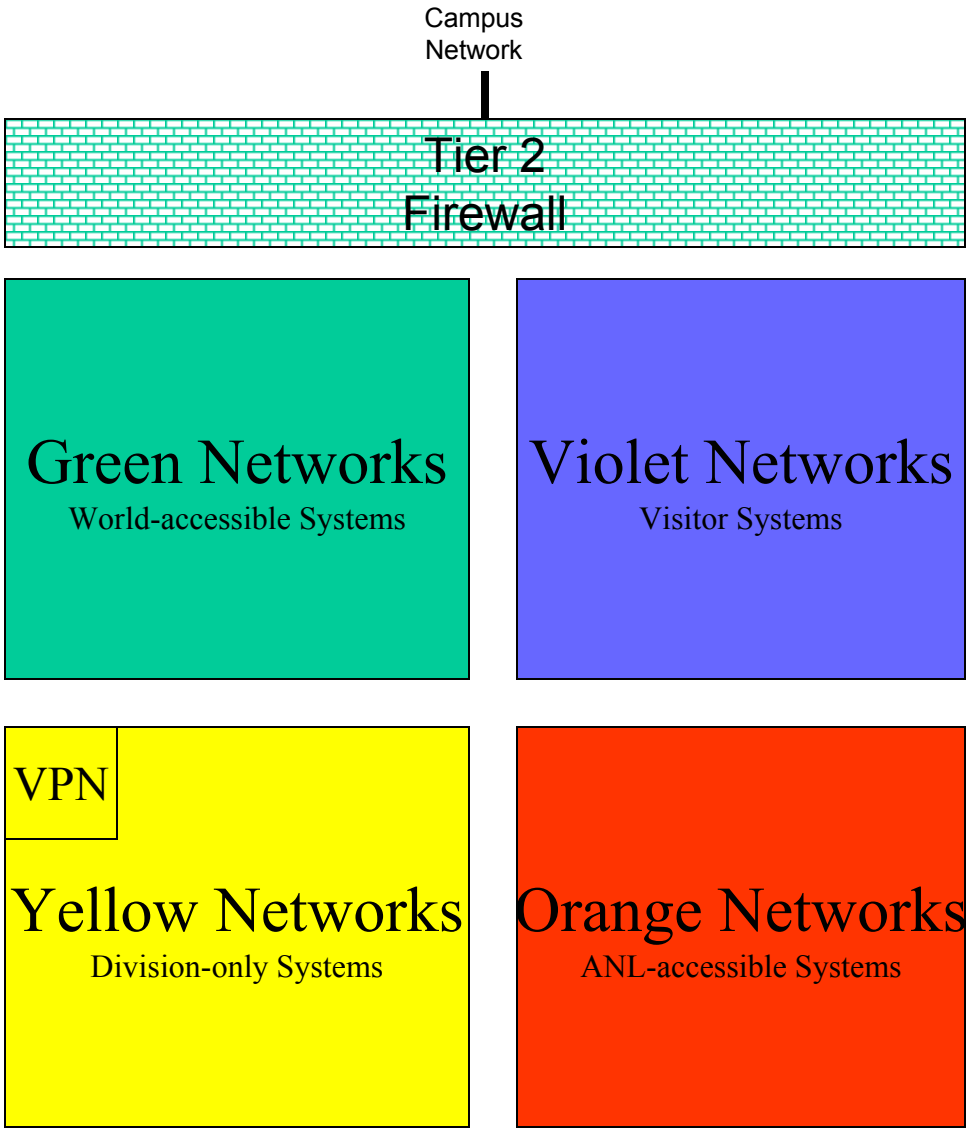
2002 / Institutionalize



- "Zones" divide the network into regions of distinctly different policy.
  - Mostly "us" and "not us".
- Conduits that enable access *between* zones must be approved by the CS-ARG.
- Zones are separated by "Tier 1 firewalls".

Network: Idealized Division Architecture

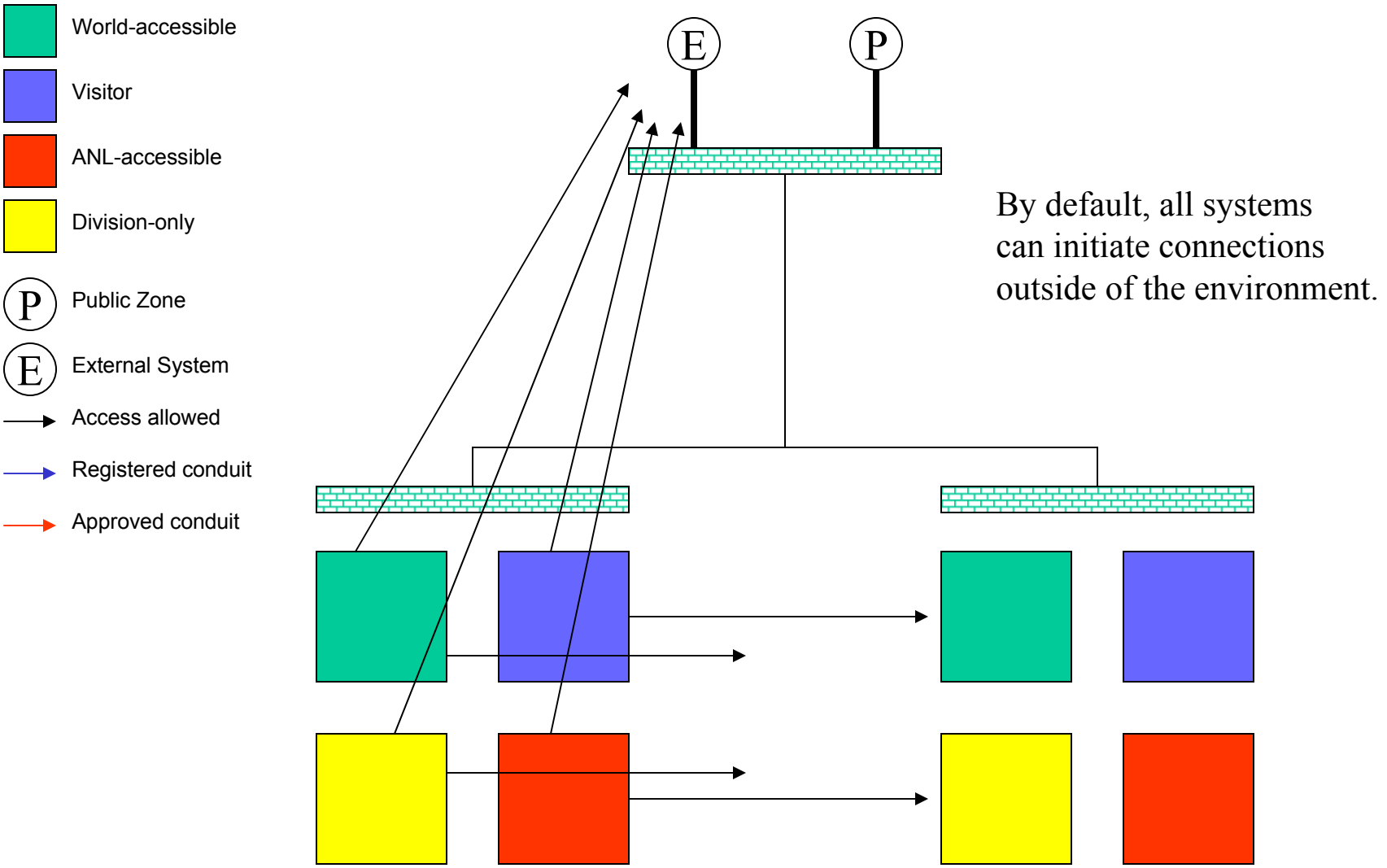
2002 / Institutionalize



- Goals:
  - Introduce network organization to divisions.
  - Make firewalls between divisions possible.
  - Make containment within a division possible.
  - Minimize the amount of pain to transition.

Tier 2 Policies – Outbound Access

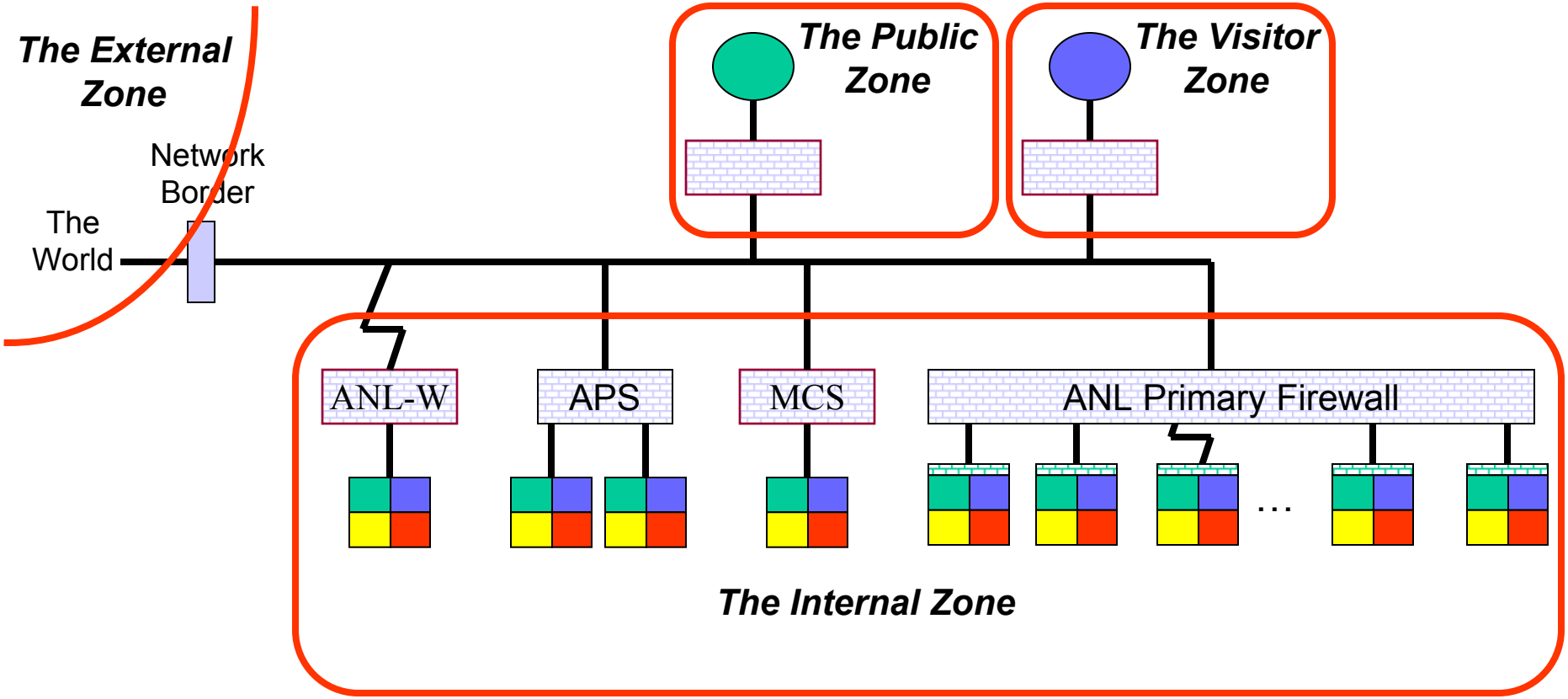
2002 / Institutionalize



By default, all systems can initiate connections outside of the environment.

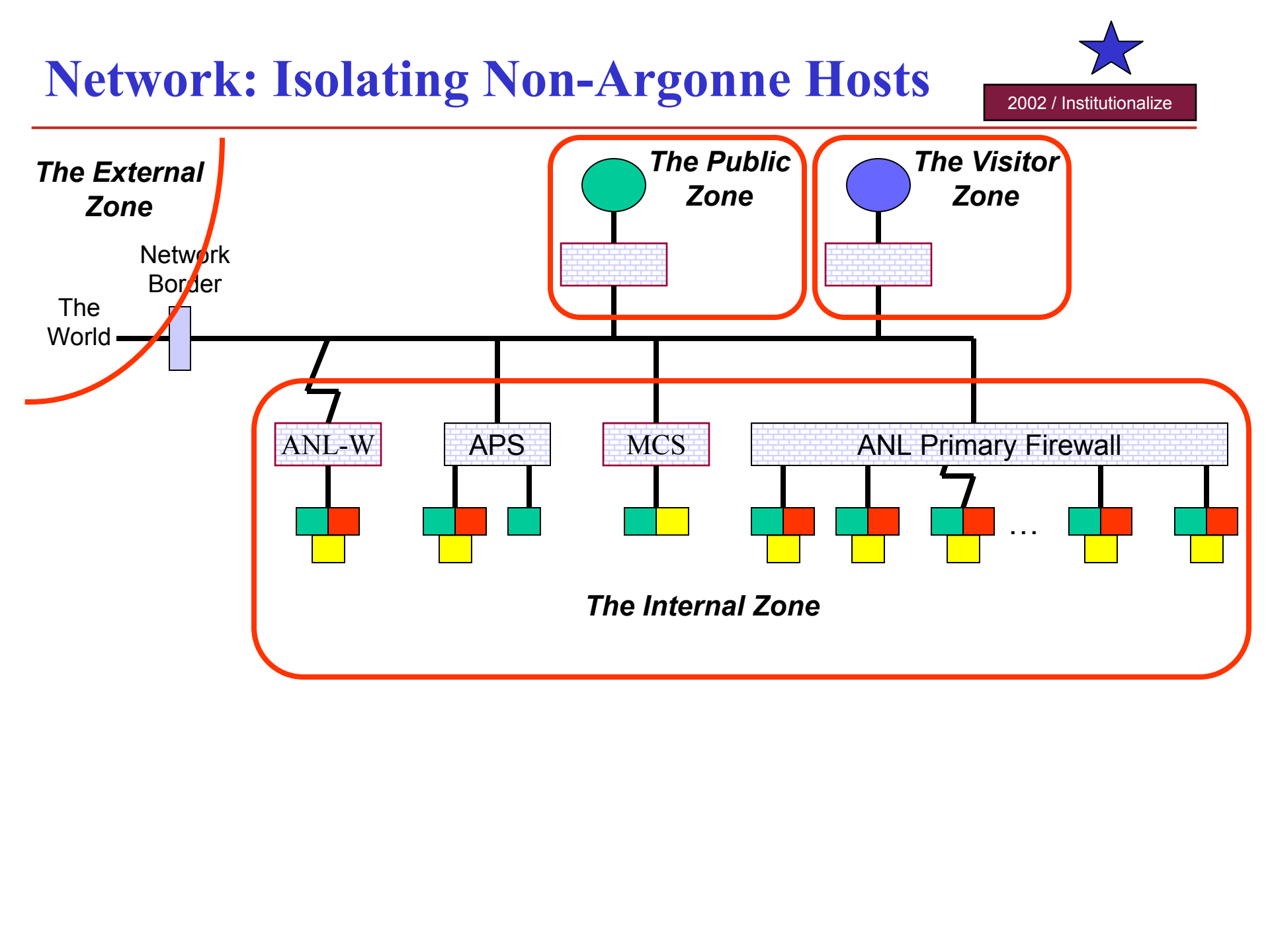
Network: Tier 2 Architecture

2002 / Institutionalize



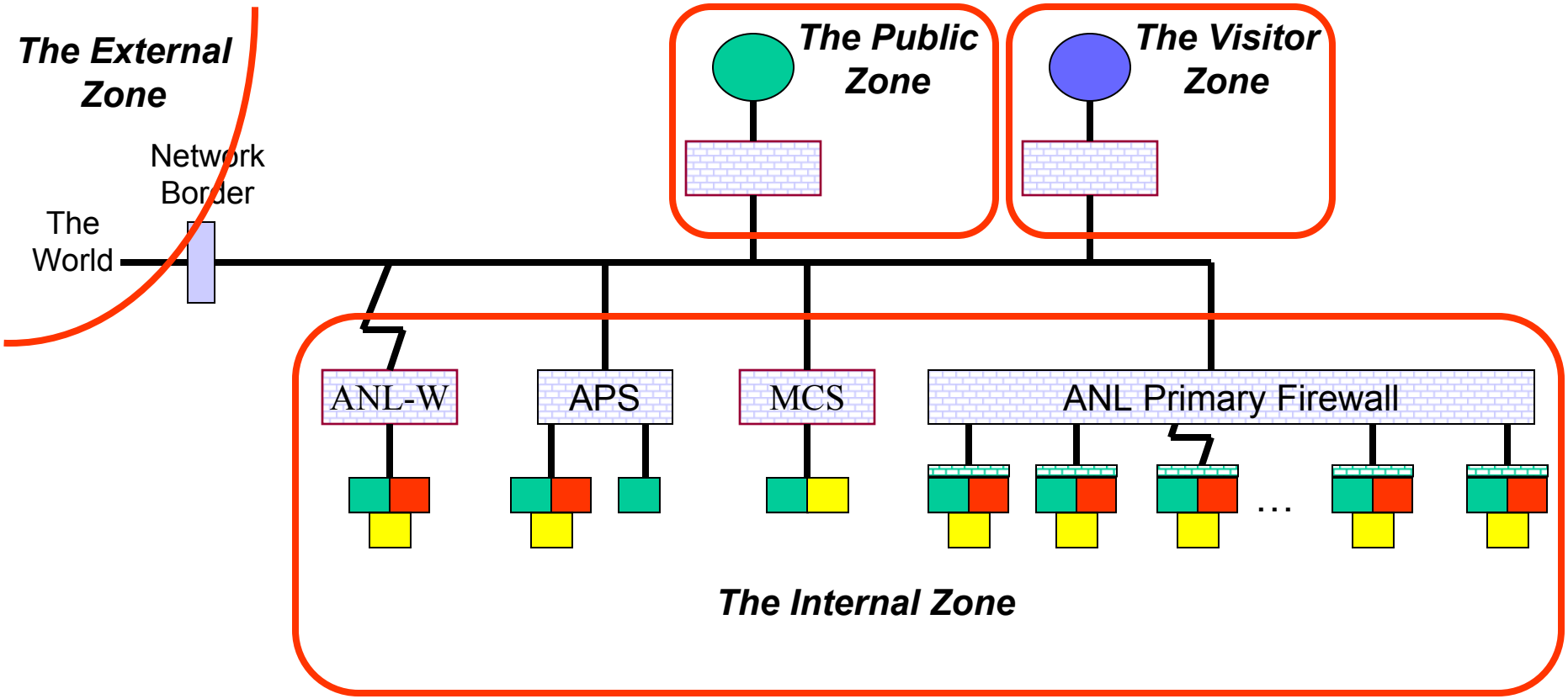
- Every network at the lab identified as a particular color.
- Divisions reorganized their networks and renumbered their hosts.

Network: Isolating Non-Argonne Hosts

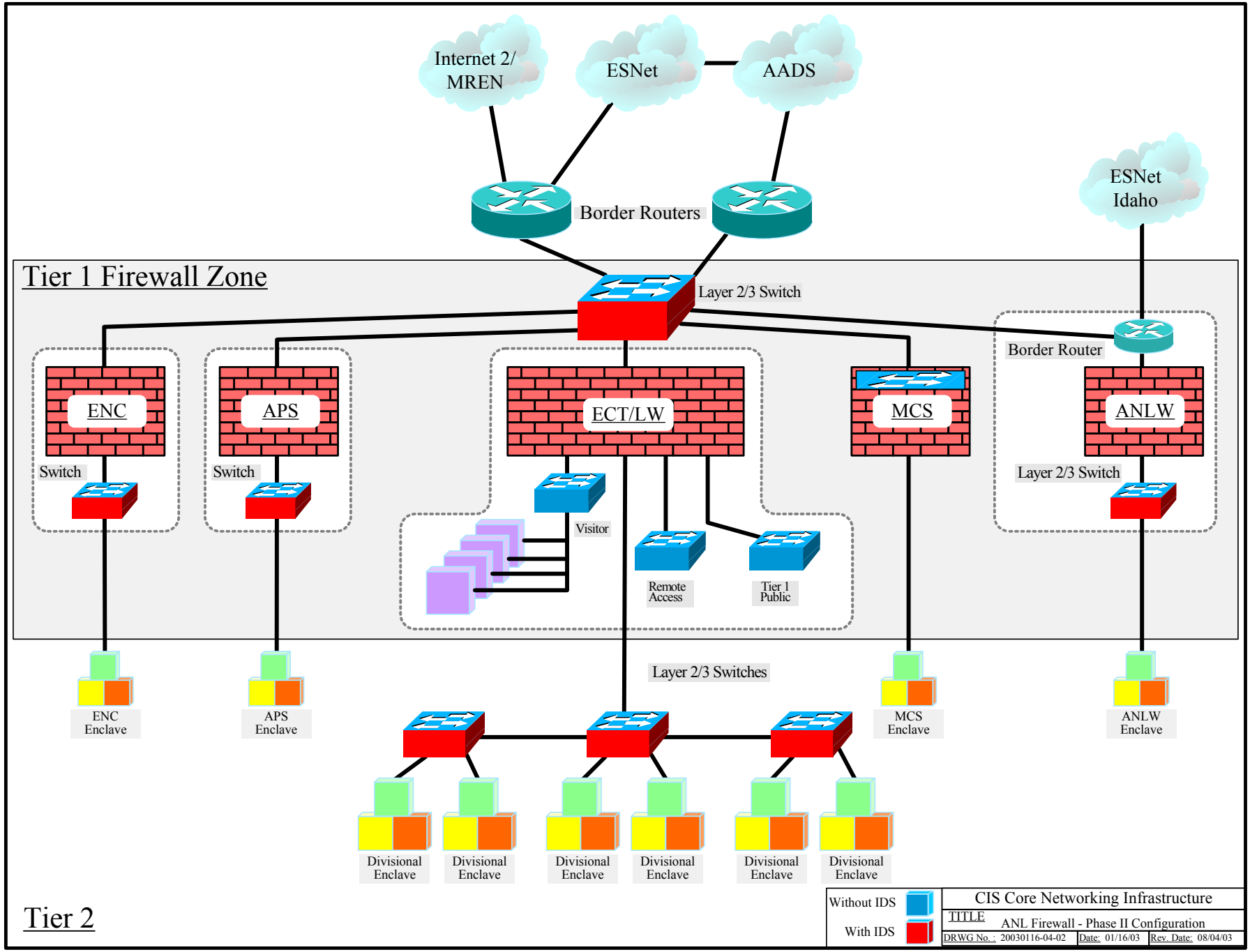


Network: Inter-Divisional Protection

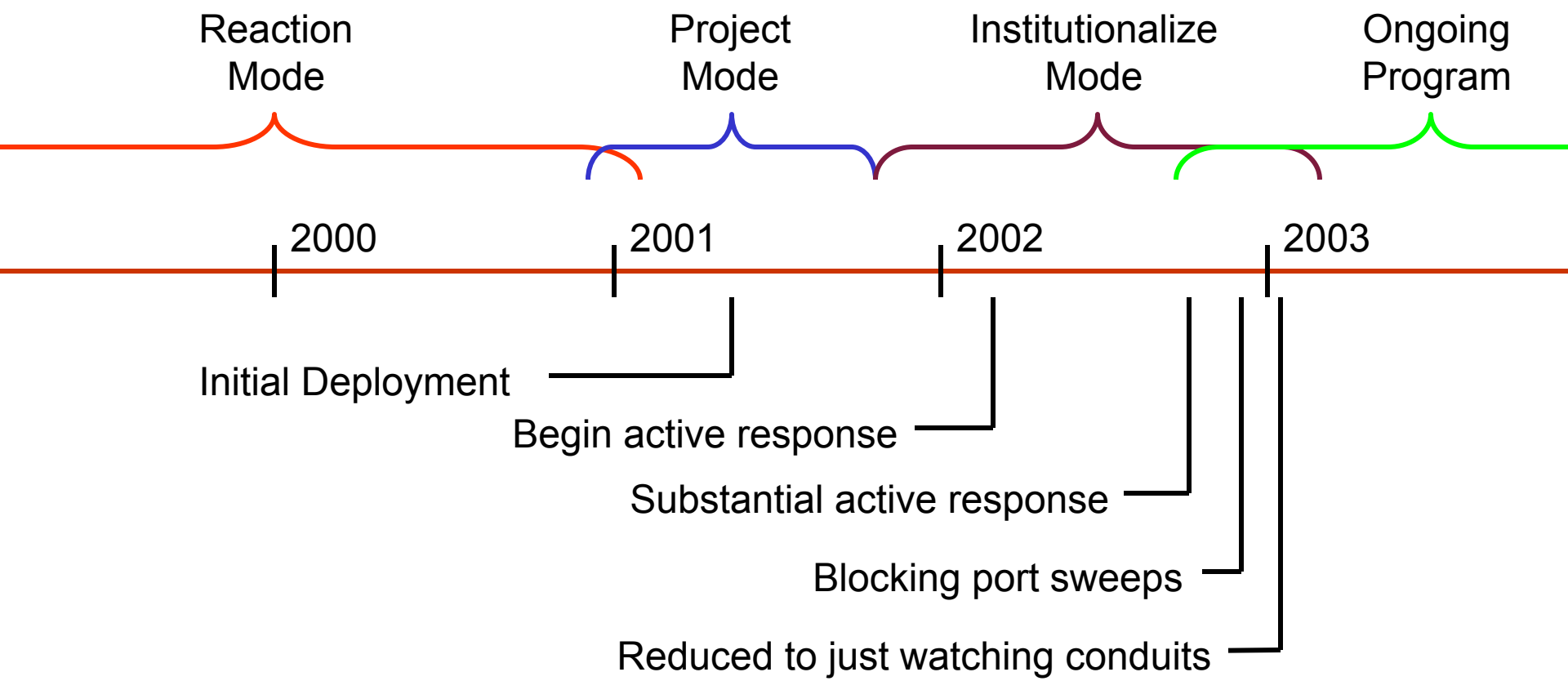
2003 / Program



- Once we had an isolated visitor zone, we required that all wireless networks be located there.


Internet 2/
MREN
ESNet
AADS
ESNet
Idaho
Border Routers
Tier 1 Firewall Zone
Layer 2/3 Switch
Border Router
ENC
APS
ECT/LW
MCS
ANLW
Switch
Switch
Layer 2/3 Switch
Visitor
Remote
Access
Tier 1
Public
Layer 2/3 Switches
ENC
Enclave
APS
Enclave
MCS
Enclave
ANLW
Enclave
Divisional
Enclave
Divisional
Enclave
Divisional
Enclave
Divisional
Enclave
Divisional
Enclave
Divisional
Enclave
Tier 2
Without IDS
With IDS
CIS Core Networking Infrastructure
TITLE
ANL Firewall - Phase II Configuration
DRWG No. : 20030116-04-02
Date: 01/16/03
Rev. Date: 08/04/03

Intrusion Detection System Timeline



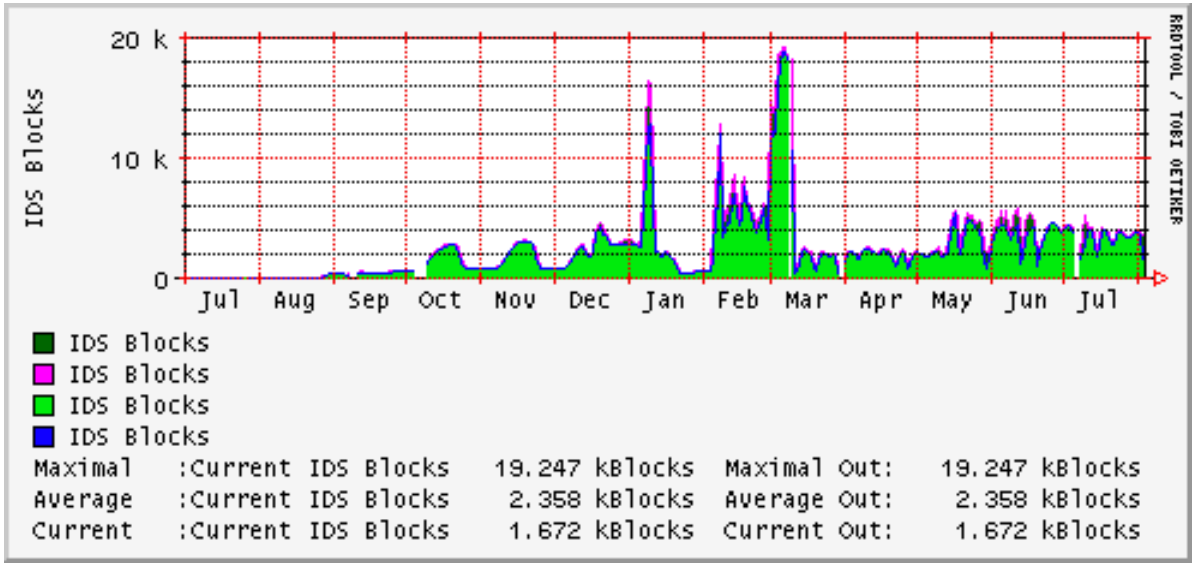
- Very useful for:
  - Detecting large-scale scans.
  - Catching viruses.
  - Looking back at “what happened”.

Issues:

- Specific target attacks.
- Encrypted data.
- Signal-to-noise and variability.

IDS Block History

2003 / Program



- Block types:
  - 24 hour blocks used on reconnaissance behavior – usually issued based on netflow analysis
  - 72 hour blocks issued on more offensive behavior (requires quiescence for block removal – NERSC model)
  - # IP's which scan > 10,000 IP's at the Lab
- Average of 3000 blocks in the firewall.
- Peak of 19000 blocks

April 2003: The Auditors Return

2003 / Program

- Initially: External scans.
  - Demonstrated that we automatically detected them.
  - Then we removed the blocks.

- On-site visit, across a 6-week period:
  - Management Review
    - Policies
    - Responsibilities
    - Risk Assessments
    - …
  - Technical Review
    - In-depth internal scans (and whatever else)
    - Visits
    - Access to all documents
    - War dialing
    - War driving
    - …

Surviving an Audit, Rule #1

- Do not piss off the auditors.

Audit Findings

2003 / Program

- "ANL-E has not fully ensured that their foreign national risk assessment processes adequately addresses specific risks associated with granting foreign nationals access to cyber systems."
- "ANL-E has not developed incident response procedures for classified information on unclassified systems, and has no formal procedure for sanitizing unclassified systems and media if they become contaminated with classified information."

- Overall: "Effective"

Moving Forward

- Continued improvements and integration
  - VIPER
  - Firewall
  - IDS usage
  - Better logging and monitoring
  - Code releases for some of the tools..?

- Making sure that policies match the requirements.

Major Concerns

- New DOE policies.
- Keeping the lab together.
  - Policies
  - Strategy
  - Implementation
  - Evolution as threats and environment change.
  - Budget.
- Technical:
  - VPNs
  - Configuration Management
  - New tech, and new vulnerabilities

Cultural Change – Have we Achieved It?

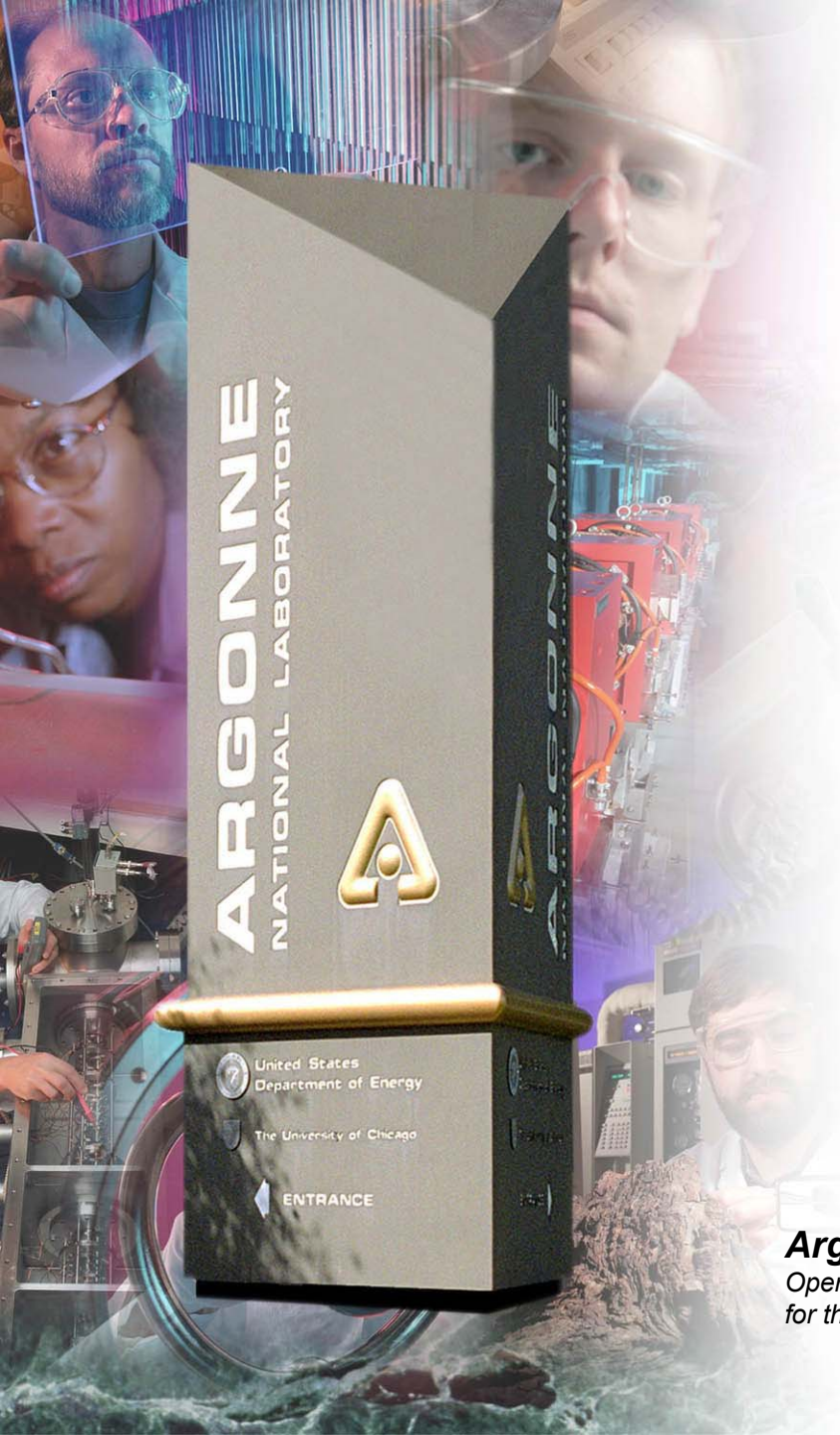
- Originally:
  - The scientific community had no desire for strong security.
- Now:
  - We've built a security environment that meets the requirements and improves the Lab's security posture - but also supports the science.
  - We became involved in the security process.

- Other indicators:
  - People know who their security rep is.
  - People know about passwords and viruses.
  - Security continues to be a topic of interest to management.

- … this will be continually challenged.

The Essential Factors In This Success

- The highest level of Lab management “got it”.
- Audits work.
  - Especially when backed up with serious downsides to audit failure.
- The project involved the entire Lab:
  - Operations
  - Management
  - Scientists
- A huge amount of hard work by the project teams and the security representatives across the Laboratory.



Security versus Science

Changing the Security Culture of a National Laboratory

Rémy Evard – evard@mcs.anl.gov

http://www.mcs.anl.gov/~evard/

Co-Authors:

Scott Pinkerton, CIS
Mike Skwarek, CIS
Gene Rackow, MCS

Argonne National Laboratory
Operated by The University of Chicago
for the U.S. Department of Energy